DESIGNLEITFADEN

EMC VSPEX-ANWENDER-COMPUTING

VMware Horizon View 6.0 und VMware vSphere mit EMC XtremIO

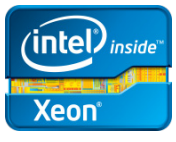
Unterstützt durch EMC Isilon, EMC VNX und EMC Datensicherheit

EMC VSPEX

Zusammenfassung

In diesem Designleitfaden wird beschrieben, wie Sie eine EMC® VSPEX®-Anwender-Computing-Lösung für VMware Horizon View aufbauen. EMC XtremIO™, EMC Isilon®, EMC VNX® und VMware vSphere stellen die Speicher- und Virtualisierungsplattformen bereit.

März 2015



EMC²

Copyright © 2014, 2015 EMC Deutschland GmbH. Alle Rechte vorbehalten.
Veröffentlicht in Deutschland.

Veröffentlicht im März 2015

EMC ist der Ansicht, dass die Informationen in dieser Veröffentlichung zum Zeitpunkt der Veröffentlichung korrekt sind. Diese Informationen können jederzeit ohne vorherige Ankündigung geändert werden.

Die Informationen in dieser Veröffentlichung werden ohne Gewähr zur Verfügung gestellt. Die EMC Corporation macht keine Zusicherungen und übernimmt keine Haftung jedweder Art im Hinblick auf die in diesem Dokument enthaltenen Informationen und schließt insbesondere jedwede implizite Haftung für die Handelsüblichkeit und die Eignung für einen bestimmten Zweck aus. Für die Nutzung, das Kopieren und die Verbreitung der in dieser Veröffentlichung beschriebenen Software von EMC ist eine entsprechende Softwarelizenz erforderlich.

EMC², EMC und das EMC Logo sind eingetragene Marken oder Marken der EMC Corporation in den USA und anderen Ländern. Alle anderen in diesem Dokument erwähnten Marken sind das Eigentum ihrer jeweiligen Inhaber.

Eine aktuelle Liste der Produkte von EMC finden Sie unter EMC Corporation Trademarks auf http://germany.emc.com.

EMC VSPEX-Anwender-Computing
VMware Horizon View 6.0 und VMware vSphere mit EMC XtremIO
Unterstützt durch EMC Isilon, EMC VNX und EMC Datensicherheit
Designleitfaden

Art.-Nr.: H13275.1

Inhalt

Kapitel 1 Einführung 9
Zweck dieses Leitfadens....10
Geschäftlicher Nutzen....10
Umfang....11
Zielgruppe....11
Terminologie....12

Kapitel 2 Bevor Sie beginnen 13
Bereitstellungsworkflow....14
Grundlegende Dokumente....14
Übersicht über die Lösungen von VSPEX....14
VSPEX-Implementierungsleitfaden....15
Handbuch zur VSPEX Proven Infrastructure....15
Leitfaden zu EMC Data Protection für VSPEX....15
Leitfaden: RSA SecurID für VSPEX-Anwender-Computing....15

Kapitel 3 Lösungsüberblick 17
Übersicht....18
VSPEX Proven Infrastructures....18
Lösungsarchitektur....19
High-Level-Architektur....19
Logische Architektur....21
Kernkomponenten....22
Desktopvirtualisierungs-Broker....23
VMware Horizon View 6.0....23
VMware View Composer....23
VMware View Persona Management....24
VMware View Storage Accelerator....24
VMware vRealize Operations Manager für Horizon View....25
Virtualisierungsebene....26
VMware vSphere....26
VMware vCenter-Server....26
VMware vSphere-Hochverfügbarkeit....26
VMware vShield Endpoint....26
Rechnerebene....26
Netzwerkebene....27
Speicherebene....27
EMC XtremIO....27

EMC Isilon 29
EMC VNX 32
Virtualisierungsmanagement 36
Datensicherheitsebene 37
Sicherheitsschicht 37
VMware Workspace-Lösung 37

Kapitel 4 Dimensionierung der Lösung 39

Übersicht 40
Referenz-Workload 40
VSPEX Private Cloud-Anforderungen: 41
Speicherlayout der Private Cloud 42
XtremIO-Arraykonfigurationen 42
Validierte XtremIO-Konfigurationen 42
XtremIO-Speicherlayout 42
Erweitern vorhandener VSPEX-Anwender-Computing-Umgebungen 43
Isilon-Konfiguration 43
VNX-Konfigurationen 44
VNX FAST VP 44
Gemeinsame VNX-Dateisysteme 44
Auswählen der geeigneten Referenzarchitektur 45
Verwenden des Arbeitsblatts für die Kundenkon-figuration 45
Auswählen einer Referenzarchitektur 47
Feinabstimmung der Hardwareress-ourcen 48
Übersicht 50

Kapitel 5 Überlegungen und Best Practices für das Lösungsdesign 51

Übersicht 52
Überlegungen zum Serverdesign 52
Best Practices für Server 53
Validierte Serverhardware 54
vSphere-Speichervirtua-lisierung 56
Richtlinien für die Arbeitsspeicherkonfiguration 57
Überlegungen zum Netzwerkdesign 59
Validierte Netzwerkhardware 60
Richtlinien für die Netzwerkkon-figuration 60
Überlegungen zum Speicherdesign 64
Überblick 64
Validierte Speicherhardware und -konfiguration 64
vSphere-Speichervirtua-lisierung 65
Hohe Verfügbarkeit und Failover 66
Virtualisierung-sebene 66
Rechnerebene 66

Netzwerkebene 67
Speicherebene 68
Profil der Validierungstests 69
Profilmerkmale 69
Virenschutz- und Anti-Malware-Plattformprofil 70
Plattformmerkmale 70
vShield-Architektur 70
VMware vRealize Operations Manager für Horizon View – Plattformprofil 70
Plattformmerkmale 70
Architektur für vRealize Operations Manager for Horizon View 71
VSPEX-Lösung für VMware Workspace 71
VMware Workspace-Kernkomponenten 71
VSPEX-Architektur für VMware Workspace 73

Kapitel 6 Referenzdokumentation 77

EMC Dokumentation 78
Andere Dokumentationen 78

Anhang A Arbeitsblatt für die Kundenkonfiguration 81

Arbeitsblatt für die Kundenkonfiguration für Anwender-Computing 82

Abbildungen

Abbildung 1. VSPEX Proven Infrastructures 19
Abbildung 2. Architektur der validierten Lösung 20
Abbildung 3. Logische Architektur 21
Abbildung 4. Isilon-Clusterkomponenten 30
Abbildung 5. Funktionen des Isilon OneFS-Betriebssystems 30
Abbildung 6. Isilon-Node-Klassen 32
Abbildung 7. Neue Unisphere Management Suite 34
Abbildung 8. Flexibilität der Rechnerebene 52
Abbildung 9. Speicherbelegung durch Hypervisor 56
Abbildung 10. Arbeitsspeichereinstellungen für virtuelle Maschinen 58
Abbildung 11. Beispiel eines XtremIO FC-Netzwerkdesigns mit hoher Verfügbarkeit 61
Abbildung 12. Beispiel eines VNX Ethernet-Netzwerkdesigns mit hoher Verfügbarkeit 62
Abbildung 13. Erforderliche Netzwerke 63
Abbildung 14. Virtuelle VMware-Laufwerktypen 66
Abbildung 15. Hohe Verfügbarkeit auf der Virtualisierungsebene 66
Abbildung 16. Redundante Netzteile 67
Abbildung 17. Hohe Verfügbarkeit der VNX-Ethernetnetzwerkebene 67
Abbildung 18. Hohe Verfügbarkeit der XtremIO-Serie 68
Abbildung 19. Layout der VMware Workspace-Architektur 72
Abbildung 20. VSPEX-Lösung für VMware Workspace: Logische Architektur 74
Abbildung 21. Druckversion des Arbeitsblatts für die Kundenkonfiguration 83

Tabelle

Tabelle 1. Terminologie 12
Tabelle 2. Bereitstellungsworkflow 14
Tabelle 3. Lösungskomponenten 22
Tabelle 4. VSPEX Anwender-Computing: Designprozess 40
Tabelle 5. Merkmale der virtuellen Referenzmaschine 40
Tabelle 6. Mindestanforderungen für den Infrastrukturserver 41
Tabelle 7. XtremIO-X-Brick-Konfigurationen 43
Tabelle 8. Ressourcenanforderungen für Benutzerdaten auf Isilon 43
Tabelle 9. Ressourcenanforderung für Benutzerdaten auf VNX 44
Tabelle 10. Beispiel für ein Arbeitsblatt für die Kundenkonfiguration 45
Tabelle 11. Ressourcen für virtuelle Referenzdesktops 47
Tabelle 12. Gesamtanzahl der Serverressourcenkomponenten 49
Tabelle 13. Serverhardware 54
Tabelle 14. Switching-Kapazität (Minimum) 60
Tabelle 15. Speicherhardware 64
Tabelle 16. Validiertes Umgebungsprofil 69
Tabelle 17. Virenschutz-Plattformmerkmale 70
Tabelle 18. Horizon View-Plattformmerkmale 71
Tabelle 19. Virtuelle OVA-Appliances 73
Tabelle 20. Mindesthardwareanforderungen für VMware Workspace 74
Tabelle 21. Arbeitsblatt für die Kundenkonfiguration 82

Kapitel 1 Einführung

In diesem Kapitel werden die folgenden Themen behandelt:

Zweck dieses Leitfadens 10

Geschäftlicher Nutzen 10

Umfang 11

Zielgruppe 11

Terminologie 12

Zweck dieses Leitfadens

Mit der EMC® VSPEX® Proven Infrastructure für das Anwender-Computing erhält der Kunde ein modernes System, mit dem eine große Zahl virtueller Desktops auf einem konsistenten Performancelevel gehostet werden kann. Diese VSPEX-Lösung für Anwender-Computing für VMware Horizon View 6.0 wird auf einer VMware vSphere-Virtualisierungsebene ausgeführt, die von der hochverfügbaren EMC XtremIO™-Produktreihe unterstützt wird, die den Speicher bereitstellt. In dieser Lösung wird die Desktopvirtualisierungsinfrastruktur auf einer VSPEX Private Cloud für VMware vSphere Proven Infrastructure ausgeführt, während die Desktops auf dedizierten Ressourcen gehostet werden.

Die von den VSPEX-Partnern definierten Rechner- und Netzwerkkomponenten sind redundant und ausreichend leistungsstark ausgelegt, um die Verarbeitungs- und Datenanforderungen einer großen virtuellen Maschinenumgebung zu erfüllen. XtremIO-Lösungen bieten Speicherplatz für virtuelle Desktops, EMC VNX®-Lösungen stellen Speicher für Benutzerdaten bereit, die EMC Avamar®-Backup- und -Recovery-Lösungen sorgen für Datensicherheit der Benutzerdaten und RSA® SecurID® bietet eine optionale sichere Benutzerauthentifizierung.

Diese VSPEX-Lösung für Anwender-Computing ist für virtuelle Desktops mit 2.500 vollständigen Clones oder 3.500 verknüpften Clones für einen X-Brick-Baustein und für virtuelle Desktops mit bis zu 1.250 vollständigen Clones oder mit bis zu 1.750 verknüpften Clones für einen Starter-X-Brick-Baustein validiert. Die validierten Konfigurationen basieren auf einem Referenzdesktop-Workload und bilden die Basis für kostengünstige, benutzerdefinierte Lösungen für Kunden.

XtremIO unterstützt Scale-out-Cluster mit bis zu sechs X-Brick-Bausteine. Jeder zusätzliche X-Brick-Baustein erhöht die Performance und virtuelle Desktopkapazität linear. XtremIO-X-Brick-Bausteine sind für den Support einer höheren Anzahl von Desktops (mit vollständigen und mit verknüpften Clones) validiert und die Zahlen der VSPEX-Validierungen gelten nur für die hier vorgestellte Lösung.

Eine Infrastruktur für Anwender-Computing oder virtuelle Desktops ist ein komplexes System. In diesem Designleitfaden wird das Design einer Lösung für Anwender-Computing mit Best Practices für VMware Horizon View für VMware vSphere mit XtremIO, EMC VNX oder EMC Isilon und EMC Datensicherheit beschrieben.

Geschäftlicher Nutzen

Geschäftliche Anwendungen werden zunehmend in konsolidierte Datenverarbeitungs-, Netzwerk- und Speicherumgebungen verlagert. Diese VSPEX-Lösung für Anwender-Computing mit VMware reduziert die Komplexität, die bei der Konfiguration der einzelnen Komponenten eines herkömmlichen Bereitstellungsmodells auftritt. Das Integrationsmanagement wird vereinfacht. Gleichzeitig bleiben die Design- und Implementierungsoptionen von Anwendungen erhalten. Zudem werden die Administration vereinheitlicht und Kontrolle und Monitoring der Prozesse ermöglicht.

Die VSPEX-Lösung für Anwender-Computing für VMware Horizon View bietet unter anderem die folgenden geschäftlichen Vorteile:

- End-to-End-Virtualisierungslösung zur Nutzung der Funktionen von einheitlichen Infrastrukturkomponenten
- Effiziente Virtualisierung für verschiedene Kunden-Anwendungsbeispiele mit virtuellen Desktops mit bis zu 2.500 vollständigen Clones oder 3.500 verknüpften Clones für einen X-Brick-Baustein und virtuellen Desktops mit bis zu 1.250 vollständigen Clones oder 1.750 verknüpften Clones für einen Starter-X-Brick-Baustein.
- Zuverlässige, flexible und skalierbare Referenzarchitekturen

Umfang

In diesem Designleitfaden wird das Design für eine einfache, effektive und flexible EMC VSPEX-Lösung für Anwender-Computing für VMware Horizon View 6.0 beschrieben. Sie bietet Beispiele für Bereitstellungen für virtuelle Desktopspeicher auf XtremIO- und Benutzerdatenspeicher auf VNX-Speicherarrays. Dieselben Prinzipien und Richtlinien gelten auch für alle VNX-Modelle, die im Rahmen des VSPEX-Programms von EMC validiert werden.

In diesem Leitfaden wird dargestellt, wie Sie Horizon View in der VSPEX-Infrastruktur dimensionieren, Ressourcen gemäß Best Practices zuweisen und alle Vorteile von VSPEX nutzen.

Die EMC Data Protection-Lösungen für die Datensicherheit in VMware Horizon View werden in einem separaten Dokument beschrieben: *Design- und Implementierungsleitfaden – EMC Backup und Recovery für VSPEX für Anwender-Computing mit VMware Horizon View*.

Die optionale Lösung für die sichere Benutzerauthentifizierung RSA SecurID für VMware Horizon View wird ebenfalls in einem separaten Dokument beschrieben, *Sicherung des EMC VSPEX-Anwender-Computing mit RSA SecurID: VMware Horizon View 5.2 und VMware vSphere 5.1 für bis zu 2.000 virtuelle Desktops – Designleitfaden*.

Zielgruppe

Dieser Leitfaden richtet sich an interne Mitarbeiter von EMC und qualifizierte EMC VSPEX-Partner. In diesem Leitfaden wird davon ausgegangen, dass VSPEX-Partner, die diese VSPEX Proven Infrastructure für VMware Horizon View bereitstellen, über die erforderliche Schulung und den entsprechenden Hintergrund verfügen, um eine Anwender-Computing-Lösung auf der Basis von Horizon View mit vSphere als Hypervisor, XtremIO-, VNX- oder Isilon-Speichersystemen und die damit verbundene Infrastruktur installieren und konfigurieren zu können.

Leser sollten außerdem mit den Infrastruktur- und Datenbanksicherheitsrichtlinien der Kundeninstallation vertraut sein.

In diesem Leitfaden werden gegebenenfalls externe Referenzen bereitgestellt. Partner, die diese Lösung implementieren, sollten mit diesen Dokumenten vertraut sein. Details finden Sie unter Grundlegende Dokumente und Kapitel 6: Referenzdokumentation.

Terminologie

In Tabelle 1 führt die in diesem Handbuch verwendete Terminologie auf.

Tabelle 1. Terminologie

Begriff	Definition
Datendeduplizierung	Eine Funktion des XtremIO-Arrays, das die Auslastung des physischen Speichers reduziert, indem redundante Datenblöcke eliminiert werden.
Vollständige Clones	Desktops, die mittels vSphere-Vorlage bereitgestellt werden
Verknüpfte Clones	Desktops, die ein gemeinsames Basis-Image innerhalb eines Desktoppools verwenden und nur wenig Platz im Speicher belegen.
Referenzarchitektur	Die validierte Architektur, die diese VSPEX-Lösung für Anwender-Computing an vier bestimmten Skalierungspunkten unterstützt – ein X-Brick-Baustein, der virtuelle Desktops mit bis zu 2.500 vollständigen Clones oder 3.500 verknüpften Clones hosten kann, und ein Starter-X-Brick-Baustein, der virtuelle Desktops mit bis zu 1.250 vollständigen Clones oder 1.750 verknüpften Clones hosten kann.
Referenz-Workload	Für VSPEX-Lösungen für Anwender-Computing ein einziger virtueller Desktop – der virtuelle Referenzdesktop – mit den Workload-Merkmalen, die unter Tabelle 5 auf Seite 40 angegeben sind. Sie können über den Vergleich der tatsächlichen Auslastung beim Kunden mit diesem Referenz-Workload ableiten, welche Referenzarchitektur als Grundlage für die VSPEX-Bereitstellung beim Kunden zu wählen ist. Details finden Sie unter Referenz-Workload.
Speicherprozessor (SP)	Die Rechnerkomponente des VNX-Speicherarrays. SPs verschieben Daten in, aus und zwischen Arrays.
Speicher-Controller (SC)	Die Rechnerkomponente des XtremIO-Speicherarrays. SCs verschieben Daten in, aus und zwischen XtremIO-Arrays.
Virtual Desktop Infrastructure (VDI)	Das Anwender-Computing entkoppelt den Desktop von der physischen Maschine. In einer VDI-Umgebung befinden sich das Desktopbetriebssystem und die Anwendungen auf einer virtuellen Maschine, die auf einem Hostcomputer ausgeführt wird. Die Daten befinden sich im gemeinsamen Speicher. Die Benutzer können von jedem Computer oder Mobilgerät aus über ein privates Netzwerk oder eine Internetverbindung auf ihren virtuellen Desktop zugreifen.
XtremIO Management Server (XMS)	Wird verwendet, um ein XtremIO-Array zu managen und als virtuelle Maschine bereitzustellen. Der XMS wird mithilfe eines Open Virtualization Appliance (OVA)-Pakets bereitgestellt.
XtremIO-Starter-X-Brick	Eine spezielle Konfiguration von XtremIO-All-Flash-Arrays, die 13 SSD-Laufwerke für diese Lösung umfasst
XtremIO X-Brick	Eine spezielle Konfiguration von vollständig flashbasierten EMC XtremIO-All-Flash-Arrays, das 25 SSD-Laufwerken für diese Lösung umfasst

Kapitel 2 Bevor Sie beginnen

In diesem Kapitel werden die folgenden Themen behandelt:

Bereitstellungsworkflow **14**

Grundlegende Dokumente **14**

Bereitstellungsworkflow

In Tabelle 2 wird der Prozessablauf dargestellt, den Sie für das Design und die Implementierung Ihrer Anwender-Computing-Lösung benötigen.[1]

Tabelle 2. Bereitstellungsworkflow

Schritt	Aktion
1	Verwenden Sie das Arbeitsblatt für die Kundenkonfiguration, um Kundenanforderungen zu erfassen. Weitere Informationen finden Sie in Anhang A in diesem Designleitfaden.
2	Verwenden Sie das EMC VSPEX-Dimensionierungstool, um die empfohlene VSPEX-Referenzarchitektur für Ihre Anwender-Computing-Lösung auf Basis der in Schritt 1 erfassten Kundenanforderungen zu ermitteln. Weitere Informationen zum Dimensionierungstool finden Sie im EMC VSPEX Sizing Tool-Portal. **Hinweis:** Sollte das Dimensionierungstool nicht zur Verfügung stehen, können Sie die Anwendung anhand der Richtlinien in Kapitel 4 dieses Designleitfadens manuell dimensionieren.
3	Mithilfe dieses Designleitfadens können Sie das endgültige Design Ihrer VSPEX-Lösung bestimmen. **Hinweis:** Sorgen Sie dafür, dass alle Ressourcenanforderungen und nicht nur die Anforderungen für das Anwender-Computing berücksichtigt werden.
4	Bestellen Sie die korrekte VSPEX-Referenzarchitektur und Proven Infrastructure. Empfehlungen zur Auswahl einer Private Cloud Proven Infrastructure finden Sie im VSPEX Proven Infrastructure-Leitfaden unter Grundlegende Dokumente .
5	Stellen Sie Ihre VSPEX-Lösung bereit, und testen Sie sie. Weitere Informationen finden Sie im VSPEX-Implementierungsleitfaden unter Grundlegende Dokumente. **Hinweis:** Die Lösung wurde von EMC mithilfe des Tools Login VSI validiert, wie in Kapitel 4 beschrieben. Unter www.loginvsi.com finden Sie hierzu weitere Informationen.

Grundlegende Dokumente

EMC empfiehlt, die folgenden Dokumente zu lesen, die Sie im Bereich „VSPEX“ im EMC Community Network, unter http://germany.emc.com oder im VSPEX Proven Infrastructure-Partnerportal finden.

Übersicht über die Lösungen von VSPEX

Lesen Sie das folgende Dokument zur VSPEX-Lösungsübersicht:

EMC VSPEX-Lösungen für Anwender-Computing mit VMware vSphere und VMware View

[1] Wenn Ihre Lösung Backup- und Recovery-Komponenten enthält, finden Sie Informationen zur Dimensionierung von Backup und Recovery sowie Implementierungsrichtlinien im *EMC Backup und Recovery für VSPEX für Anwender-Computing mit VMware View – Design- und Implementierungsleitfaden*.

VSPEX-Implementierungsleitfaden	Lesen Sie den folgenden VSPEX-Implementierungsleitfaden: *EMC VSPEX Anwender-Computing: VMware Horizon View 6.0 und VMware vSphere mit EMC XtremIO*
Handbuch zur VSPEX Proven Infrastructure	Details finden Sie im Proven Infrastructure-Leitfaden *EMC VSPEX Private Cloud: VMware vSphere 5.5 für bis zu 1.000 virtuelle Maschinen*
Leitfaden zu EMC Data Protection für VSPEX	Details finden Sie im *Design- und Implementierungsleitfaden – EMC Backup und Recovery für VSPEX für Anwender-Computing mit VMware View*
Leitfaden: RSA SecurID für VSPEX-Anwender-Computing	Weitere Informationen finden Sie im *Sicherung des EMC VSPEX-Anwender-Computings mit RSA SecurID: VMware Horizon View 5.2 mit VMware vSphere 5.1 für bis zu 2.000 virtuelle Desktops – Designleitfaden*

Kapitel 3 Lösungsüberblick

In diesem Kapitel werden die folgenden Themen behandelt:

Übersicht 18
VSPEX Proven Infrastructures 18
Lösungsarchitektur 19
Kernkomponenten 22
Desktopvirtualisierungs-Broker 23
Virtualisierungsebene 26
Rechnerebene 26
Netzwerkebene 27
Speicherebene 27
Datensicherheitsebene 37
Sicherheitsschicht 37
VMware Workspace-Lösung 37

Übersicht

In diesem Kapitel finden Sie einen Überblick über die VSPEX-Lösung für Anwender-Computing für VMware Horizon View mit VMware vSphere und die wichtigsten Lösungstechnologien. Die Lösung wurde von EMC entwickelt und erprobt und bietet die erforderlichen Ressourcen für Virtualisierung, Server, Netzwerk, Speicher und Backup für den Support von Referenzkonfigurationen für die folgenden validierten X-Brick-Bausteinkonfigurationen des XtremIO-All-Flash-Arrays:

- XtremIO-Starter-X-Brick-Baustein: enthält 13 SSD-Laufwerke und unterstützt virtuelle Desktops mit bis zu 1.250 vollständigen Clones oder 1.750 verknüpften Clones.
- XtremIO-X-Brick-Baustein: enthält 25 SSD-Laufwerke und unterstützt virtuelle Desktops mit bis zu 2.500 vollständigen Clones oder 3.500 verknüpften Clones.

XtremIO-X-Brick-Bausteine sind für den Support einer höheren Anzahl von Desktops (mit vollständigen und mit verknüpften Clones) validiert und die Zahlen der VSPEX-Validierungen gelten nur für diese Lösung.

Obwohl die Infrastrukturkomponenten für die Desktopvirtualisierung der Lösung in Abbildung 3 dafür entwickelt wurden, in einer VSPEX Private Cloud ausgeführt zu werden, umfassen die Referenzarchitekturen keine Konfigurationsdetails für die zugrunde liegende Proven Infrastructure. Informationen zur Konfiguration der erforderlichen Infrastruktur finden Sie im VSPEX Proven Infrastructure-Leitfaden unter Grundlegende Dokumente.

VSPEX Proven Infrastructures

EMC hat gemeinsam mit den branchenführenden Anbietern von IT-Infrastrukturen eine umfassende Virtualisierungslösung entwickelt, die die Bereitstellung der Private Cloud und von virtuellen VMware Horizon View-Desktops beschleunigt. Mit VSPEX sind Kunden in der Lage, die Transformation der IT durch schnellere Bereitstellung, verbesserte Anwenderfreundlichkeit, größere Auswahl, höhere Effizienz und weniger Risiko zu beschleunigen. Dadurch wird die Erstellung der IT-Infrastruktur vereinfacht.

Die VSPEX-Validierung durch EMC ermöglicht eine zuverlässige Performance und ermöglicht Kunden die Auswahl von Technologien, die ihre vorhandene oder neu erworbene IT-Infrastruktur nutzen und so den Planungs-, Dimensionierungs- und Konfigurationsaufwand vermeiden. VSPEX stellt eine virtuelle Infrastruktur für Kunden bereit, die die Einfachheit von echten konvergenten Infrastrukturen und gleichzeitig mehr Auswahlmöglichkeiten bei den einzelnen Komponenten erreichen möchten.

VSPEX Proven Infrastructures, wie in Abbildung 1 gezeigt, sind modulare und virtualisierte Infrastrukturen, die von EMC validiert und von EMC VSPEX-Partnern geliefert werden. Sie umfassen die Virtualisierungs-, Server-, Netzwerk-, Speicher- und Backupebene. Partner können die Virtualisierungs-, Server- und Netzwerktechnologien auswählen, die am besten zur Umgebung eines Kunden passen. Gleichzeitig stellen die Speichersysteme der hoch verfügbaren XtremIO- und VNX-Produktreihe und EMC Datensicherheitstechnologien die Speicher- und Backupebene zur Verfügung.

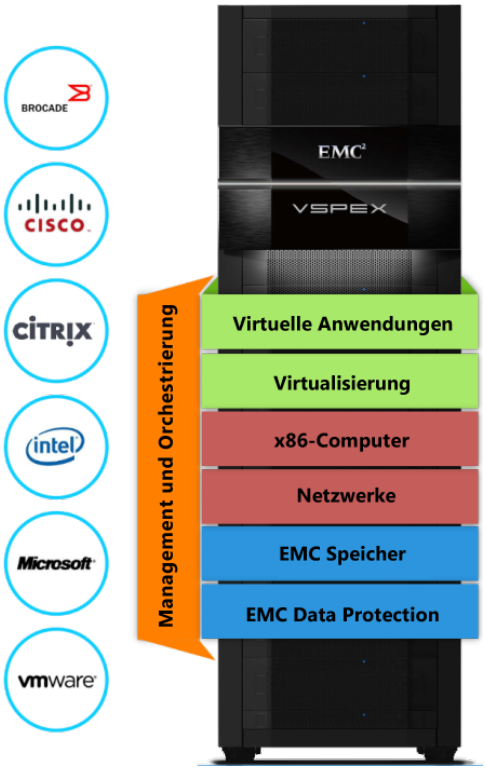


Abbildung 1. VSPEX Proven Infrastructures

Lösungsarchitektur

High-Level-Architektur

Die EMC VSPEX-Lösung für Anwender-Computing für VMware Horizon View bietet eine vollständige Systemarchitektur mit zwei XtremIO-X-Brick-Bausteinkonfigurationen. Ein XBrick-Baustein kann virtuelle Desktops mit bis zu 2.500 vollständigen Clones oder 3.500 verknüpften Clones hosten, ein Starter-X-Brick-Baustein kann virtuelle Desktops mit bis zu 1.250 vollständigen Clones oder 1.750 verknüpften Clones hosten. Die Lösung unterstützt Blockspeicher auf XtremIO für virtuelle Desktops und optionale Dateispeicher auf Isilon oder VNX für Benutzerdaten.

XtremIO-X-Brick-Bausteine sind für den Support einer höheren Anzahl von Desktops mit vollständigen und mit verknüpften Clones validiert und die Zahlen der VSPEX-Validierungen gelten nur für diese Lösung.

Abbildung 2 zeigt die allgemeine Architektur der validierten Lösung.

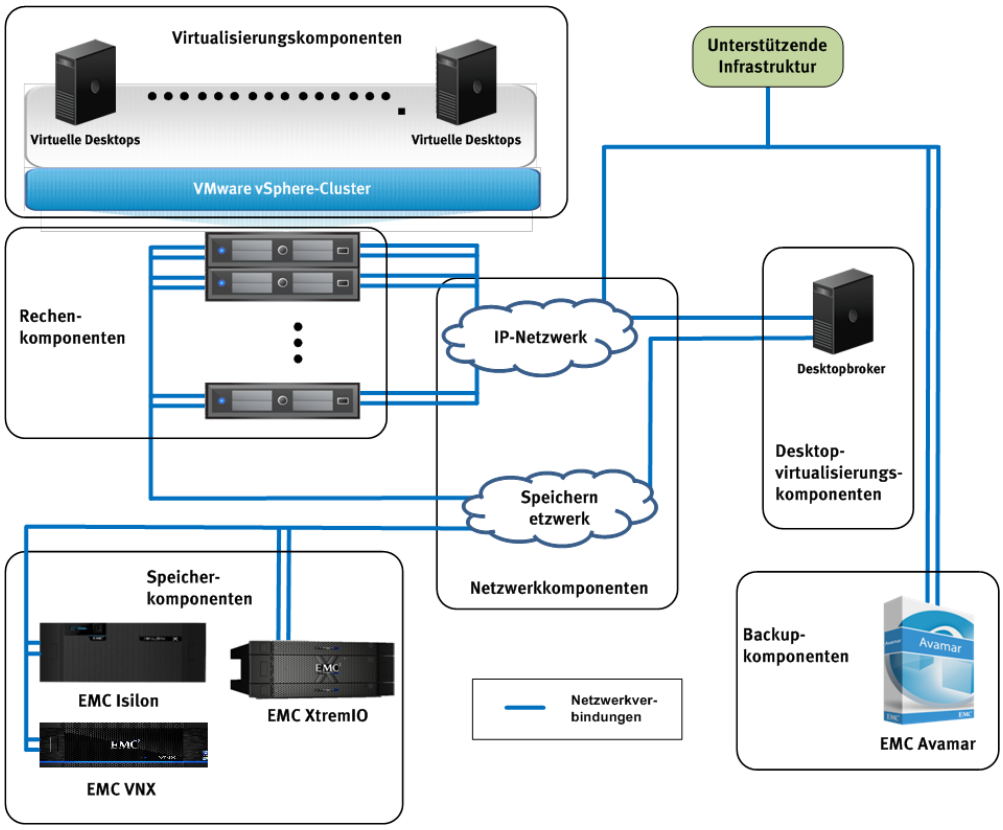


Abbildung 2. Architektur der validierten Lösung

Diese Lösung verwendet XtremIO, Isilon oder VNX und VMware vSphere für die Bereitstellung der Speicher- und Virtualisierungsplattformen für von VMware Horizon View Composer bereitgestellte virtuelle Microsoft Windows 7- oder Windows 8.1-Desktops.

Für diese Lösung haben wir[2] das XtremIO-Array in mehreren Konfigurationen bereitgestellt, um bis zu 3.500 virtuelle Desktops zu unterstützen. Wir haben zwei XtremIO-Arrays getestet: ein Starter-X-Brick, der virtuelle Desktops mit bis zu 1.250 vollständigen Clones oder 1.750 verknüpften Clones hosten kann, und ein X-Brick, der virtuelle Desktops mit bis zu 2.500 vollständigen Clones oder 3.500 verknüpften-Clones hosten kann. Wir haben auch Isilon- und VNX-Arrays für das Hosten von Benutzerdaten bereitgestellt.

Das hochverfügbare XtremIO-Array stellt den Speicher für die virtuellen Desktops bereit. Die Infrastrukturservices für die Lösung, die in Abbildung 3 dargestellt sind, können durch eine vorhandene Infrastruktur am Kundenstandort, durch die VSPEX Private Cloud oder durch die Bereitstellung der Services als dedizierte Ressourcen im Rahmen der Lösung bereitgestellt werden. Für die virtuellen Desktops, die in Abbildung 3 dargestellt werden, sind dedizierte Anwender-Computing-Ressourcen erforderlich. Eine Ausführung des Clusters in einer VSPEX Private Cloud ist nicht vorgesehen.

[2] In diesem Leitfaden bezieht sich „wir“ auf das EMC Solutions Engineering-Team, das die Lösung validierte.

Die Planung und das Design der Speicherinfrastruktur für eine Horizon View-Umgebung sind ein wichtiger Schritt, da der gemeinsame Speicher in der Lage sein muss, große Belastungsspitzen bei I/O-Vorgängen abzufangen. Diese Belastungsspitzen können zu Phasen mit einer unregelmäßigen und unzuverlässigen Performance der virtuellen Desktops führen. Benutzer mögen sich an eine langsame Performance gewöhnen, aber eine unzuverlässige Performance führt zu Frustration und verringert die Effizienz.

Für eine zuverlässige Performance in Anwender-Computing-Lösungen muss das Speichersystem die I/O-Spitzenlast der Clients bei minimaler Antwortzeit verarbeiten können. Diese Lösung verwendet das XtremIO-Array, um die von Kunden benötigten Antwortzeiten unter einer Millisekunde zu ermöglichen, während die Funktionen der Echtzeit-Inline-Deduplizierung und Inline-Komprimierung der Plattform die benötigten physischen Speichermedien verringern.

EMC Data Protection-Lösungen ermöglichen den Schutz von Benutzerdaten und die Wiederherstellbarkeit durch Anwender. Dafür werden in dieser Horizon View-Lösung Avamar und der damit verbundene Desktopclient verwendet.

Logische Architektur

Die EMC VSPEX-Lösung für Anwender-Computing für VMware Horizon View unterstützt Blockspeicher auf XtremIO für die virtuellen Desktops. Abbildung 3 zeigt die logische Architektur der Lösung.

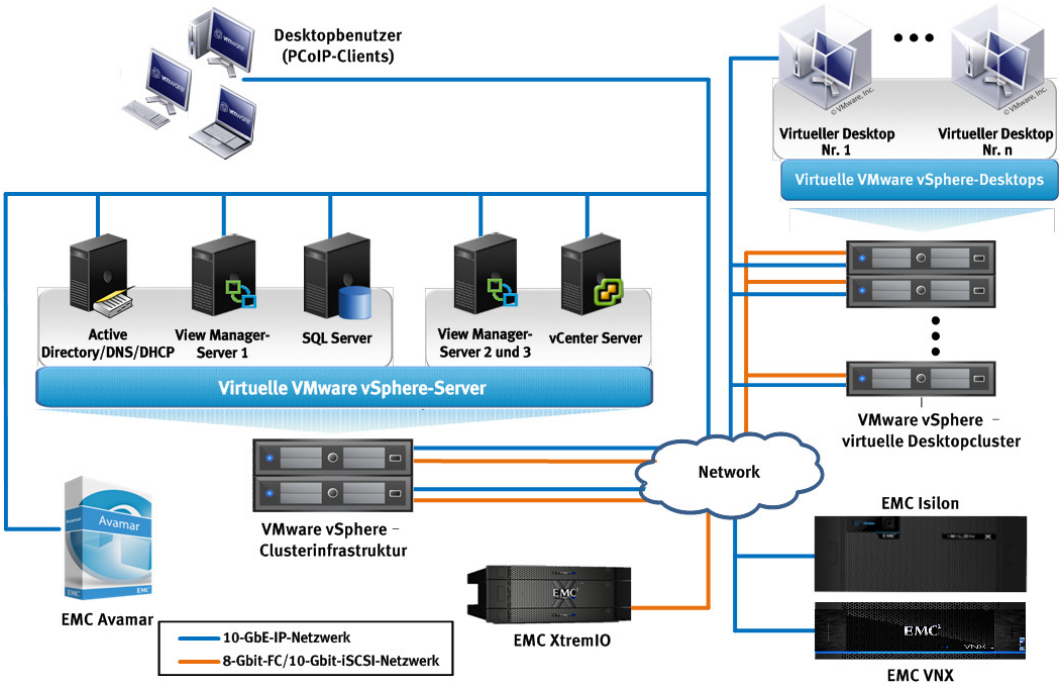


Abbildung 3. Logische Architektur

Diese Lösung verwendet zwei Netzwerke: ein Speichernetzwerk (8-Gbit-FC oder 10-GbE-iSCSI) zur Bereitstellung von virtuellen Desktop- und virtuellen Serverbetriebssystemdaten sowie ein 10-Gbit-Ethernetnetzwerk für den übrigen Datenverkehr. Das Speichernetzwerk verwendet 8-Gbit-Fibre Channel (FC) oder 10-Gbit-Ethernet mit iSCSI-Protokoll.

Hinweis: Die Lösung unterstützt darüber hinaus 1-Gbit-Ethernet, falls die Bandbreitenerfordernisse erfüllt werden.

Kernkomponenten

In diesem Abschnitt finden Sie einen Überblick über die wichtigsten in dieser Lösung verwendeten Technologien, die in Tabelle 3 dargestellt sind.

Tabelle 3. Lösungskomponenten

Komponente	Beschreibung
Desktopvirtualisierungs-Broker	Managt das Provisioning, die Zuweisung, die Wartung und das Entfernen der virtuellen Desktop-Images, die den Benutzern bereitgestellt werden. Diese Software ermöglicht die Erstellung von Desktop-Images nach Bedarf und eine Image-Wartung ohne Beeinträchtigung der Benutzerproduktivität und verhindert ein unkontrolliertes Wachstum der Umgebung. VMware Horizon View 6.0 ist der Desktop-Broker in dieser Lösung.
Virtualisierungsebene	Er entkoppelt physische Ressourcen von den Anwendungen, die sie verwenden. Die Ansicht der Ressourcenverfügbarkeit für die Anwendung ist nicht an die Hardware gebunden. Auf diese Weise können viele Hauptfunktionen des Anwender-Computing-Konzepts genutzt werden. In dieser Lösung wird VMware vSphere für die Virtualisierungsebene verwendet.
Rechnerebene	Es stellt CPU- und Speicherressourcen für die Virtualisierungsebene und für die in der Infrastruktur ausgeführten Anwendungen zur Verfügung. Das VSPEX-Programm definiert die Mindestanzahl der auf der Rechnerebene benötigten Ressourcen, gibt aber dem Benutzer die Möglichkeit, die Lösung auf jeder Serverhardware zu implementieren, die die Anforderungen erfüllt.
NetzwerkebeneNetzwerkebene	Verbindet die Benutzer mit den benötigten Ressourcen und die Speicherebene mit der Rechnerebene. Das VSPEX-Programm definiert die Mindestanzahl der für die Lösung erforderlichen Netzwerkports und stellt allgemeine Richtlinien zur Netzwerkarchitektur zur Verfügung, ermöglicht dem Kunden jedoch die Implementierung der Lösung mit jeder beliebigen Netzwerkhardware, die die Anforderungen erfüllt.
Speicherebene	Die Speicherebene ist eine wichtige Ressource für die Implementierung der Anwender-Computing-Umgebung und muss hohe Aktivitätsbelastungsspitzen auffangen können, ohne die Benutzererfahrung zu beeinträchtigen. Diese Lösung verwendet Arrays der XtremIO- und Isilon- oder VNX-Serien, um diesen Workload zu bewältigen.
Datensicherheits	Eine optionale Komponente, die Datensicherheit bietet, wenn Daten im Primärsystem gelöscht oder beschädigt wurden oder nicht mehr verwendet werden können. Diese Lösung verwendet Avamar für die Datensicherheit.
Sicherheitsschicht	Eine optionale Komponente, die dem Kunden Optionen zur Steuerung des Zugriffs auf die Umgebung bereitstellt und dafür sorgt, dass ausschließlich autorisierte Benutzer auf das System zugreifen können. Diese Lösung verwendet RSA SecurID, um Benutzerauthentifizierung bereitzustellen.
VMware Workspace-	Optionaler Support für VMware Workspace-Bereitstellungen

Desktopvirtualisierungs-Broker

Die Desktopvirtualisierung verkapselt und hostet Desktopservices auf zentralen Rechnerressourcen in Remoterechenzentren. Damit können sich Anwender von verschiedenen Geräten mit ihren virtuellen Desktops verbinden. Zu diesen Geräten können Desktops, Laptops, Thin Clients, Zero Clients, Smartphones und Tablets gehören.

Bei dieser Lösung haben wir VMware Horizon View für die Bereitstellung, Verwaltung, Vermittlung und Überwachung der Desktopvirtualisierungsumgebung verwendet.

VMware Horizon View 6.0

VMware Horizon View ist eine führende Desktopvirtualisierungslösung, die Anwendern Desktopservices aus der Cloud bietet. VMware Horizon View 6.0 kann in vSphere integriert werden und bietet die folgenden Vorteile:

- Speicherressourcenoptimierung: View Composer optimiert die Speicherauslastung und Performance durch Reduzierung der Stellfläche von virtuellen Desktops.
- Support für Thin Provisioning: Horizon View 6.0 ermöglicht bei der Bereitstellung virtueller Desktops die Zuweisung von Speicherressourcen. Dies führt zu einer besseren Auslastung der Speicherinfrastruktur und niedrigeren Investitions- und Betriebsausgaben.
- Rückgewinnung von Speicherplatz für virtuelle Maschinen auf Desktops: Horizon View 6.0 kann freien Speicherplatz auf virtuellen Windows 8.1-Desktops wiedergewinnen. Dadurch wird sichergestellt, dass der für die verknüpften Clone-Desktops erforderliche Speicherplatz im gesamten Lebenszyklus des Desktops auf ein Minimum reduziert wird.

Die Version Horizon View 6.0 führt die folgenden Verbesserungen für mehr Benutzerfreundlichkeit ein:

- Möglichkeit, Anwendungen direkt an View-Clients über Microsoft Windows RDS-Server zu streamen
- Möglichkeit, standortübergreifende, verbundene View-Pods zu erstellen, um Disaster Recovery oder Lastausgleichinitiativen zu unterstützen
- Einen virtuellen Grafikprozessor (GPU) zum Support von hardwarebeschleunigten 3D-Grafiken
- Desktopbedienung über HTML5 sowie iOS- und Android-Anwendungen

In den Versionshinweisen für VMware Horizon View 6.0 finden Sie weitere Informationen.

Die VMware Horizon View-Editionen sind Lösungspakete, die VMware vSphere Desktop Edition und vCenter Desktop Server umfassen. Für die Lösungsvalidierung haben wir VMware Horizon Enterprise Edition bereitgestellt, welches vCenter Desktop, vSphere Desktop, View Manager, View Composer, View Persona Management, Workspace und VMware ThinApp umfasst.

VMware View Composer

VMware View Composer arbeitet direkt mit vCenter Server zusammen, um den Status der virtuellen Desktops bei Verwendung von verknüpften Clones bereitzustellen, anzupassen und beizubehalten.

View Composer aktiviert außerdem die folgenden Funktionen:

- Support für Tiered Storage, um die Verwendung dedizierter Speicherressourcen für die Platzierung des schreibgeschützten Replikats und der Laufwerks-Images der verknüpften Clones zu ermöglichen
- Optionaler eigenständiger View Composer-Server, um die Auswirkung von virtuellem Desktop-Provisioning und Wartungsvorgängen auf dem vCenter-Server zu minimieren

Für diese Lösung wurde View Composer verwendet, um dedizierte virtuelle Desktops, auf denen Windows 7 oder Windows 8.1 ausgeführt wird, als verknüpfte Clones bereitzustellen.

VMware View Persona Management

VMware View Persona Management behält Benutzerprofile bei und synchronisiert diese mit einem Remote-Profil-Repository. Für View Persona Management ist keine Konfiguration von Windows-Roaming-Profilen erforderlich, wodurch sich die Notwendigkeit der Verwendung von Active Directory für das Management von Horizon View-Benutzerprofilen erübrigt.

View Persona Management bietet im Vergleich zu herkömmlichen Windows-Roaming-Profilen die folgenden Vorteile:

- Horizon View lädt das Remoteprofil eines Benutzers dynamisch herunter, wenn sich dieser bei einem View-Desktop anmeldet.
- Während der Anmeldung lädt Horizon View nur die Dateien herunter, die für Windows erforderlich sind, z. B. Registry-Dateien des Benutzers. Andere Dateien werden auf den lokalen Desktop kopiert, wenn der Benutzer oder eine Anwendung diese aus dem lokalen Profilordner öffnet.
- Horizon View kopiert letzte Änderungen im lokalen Profil in das Remote Repository. Das Zeitintervall für die Kopien kann beliebig konfiguriert werden.
- Während der Abmeldung kopiert Horizon View nur die Dateien, die seit der letzten Replikation geändert wurden, in das Remote-Repository.
- View Persona Management kann so konfiguriert werden, dass Benutzerprofile in einem sicheren und zentralen Repository gespeichert werden.

VMware View Storage Accelerator

VMware View Storage Accelerator reduziert die mit virtuellen Desktops verbundene Speicherlast, indem die gemeinsamen Blöcke von Desktop Images im lokalen vSphere-Hostspeicher zwischengespeichert werden. Dafür nutzt Storage Accelerator Content Based Read Cache (CBRC), der im vSphere-Hypervisor implementiert wird.

Ist diese Funktion für die virtuellen Horizon View-Desktoppools aktiviert, durchsucht der Host-Hypervisor die Blöcke der Speicherlaufwerke, um Auszüge der Blockinhalte zu generieren. Diese Blöcke werden in den hostbasierten CBRC zwischengespeichert, wenn der Hypervisor sie liest. Nachfolgende Lesezugriffe auf Blöcke mit demselben Auszug werden direkt vom speicherinternen Cache verarbeitet. Dies sorgt für eine deutlich bessere Performance der virtuellen Desktops, insbesondere bei Boot Storms oder bei Spitzenlasten während des Starts, der Benutzeranmeldung oder Virenschutzprüfung, wenn eine große Anzahl von Blöcken mit gleichen Inhalten gelesen wird.

VMware vRealize Operations Manager für Horizon View

VMware vRealize Operations Manager für Horizon View bietet umfassende Einblicke in die Integrität, Performance und Effizienz der virtuellen Desktopinfrastruktur (VDI)-Umgebungen. Er ermöglicht es Desktopadministratoren, proaktiv für eine optimale Anwendererfahrung zu sorgen, Vorfälle zu verhindern und Engpässe zu eliminieren. Diese Version von vRealize Operations Manager ist für VMware Horizon View konzipiert, verbessert die IT-Produktivität und senkt die Gesamtbetriebskosten von VDI-Umgebungen.

Zu den wichtigsten Funktionen zählen:

- Patentierte Selbstlern-Analysefunktionen, die sich an Ihre Umgebung anpassen und kontinuierlich Tausende von Messwerten bezüglich der Server-, Speicher-, Netzwerk- und Anwenderperformance analysieren.
- Umfassende Dashboards zur Vereinfachung des Performance- und Integritätsmonitoring, Identifizierung von Engpässen und zur Verbesserung der Horizon View-Infrastruktureffizienz
- Dynamische Schwellenwerte und „Smart Alerts“, die Administratoren warnen und spezifischere Informationen zu drohenden Performanceproblemen liefern
- Automatisierte Ursachenanalyse, Sitzungssuche und Ereigniskorrelation für eine schnellere Behebung von Anwenderproblemen.
- Integrierter Ansatz bezüglich Performance, Kapazität und Konfiguration, welcher das ganzheitliche Management von VDI-Vorgängen unterstützt
- Design und Optimierungen speziell für VMware Horizon View

Virtualisierungsebene

VMware vSphere

VMware vSphere ist die marktführende Virtualisierungsplattform. Anwender profitieren von der Flexibilität und den Kosteneinsparungen durch die Lösung aufgrund der Konsolidierung großer, ineffizienter Serverfarmen in anpassungsfähige, zuverlässige Infrastrukturen. Die VMware vSphere-Kernkomponenten sind der VMware vSphere-Hypervisor und VMware vCenter Server.

Diese Lösung nutzt VMware vSphere Desktop Edition, die für Kunden ausgelegt ist, die vSphere-Lizenzen nur für Desktopvirtualisierung erwerben möchten. vSphere Desktop bietet ein umfassendes Angebot an Funktionen der vSphere Enterprise Plus Edition und eine unbegrenzte vRAM-Berechtigung.

VMware vCenter-Server

VMware vCenter Server ist eine zentrale Plattform für das Management der vSphere-Umgebungen. Sie stellt Administratoren eine einzige Oberfläche für alle Monitoring-, Management- und Wartungsaufgaben im Zusammenhang mit der virtuellen Infrastruktur zur Verfügung.

vCenter ist auch für das Management von erweiterten Funktionen wie vSphere High Availability (HA), vSphere Distributed Resource Scheduler (DRS), vSphere vMotion und vSphere Update Manager verantwortlich.

VMware vSphere-Hochverfügbarkeit

VMware vSphere HA bietet einheitlichen, kostengünstigen Failover-Schutz vor Hardware- und Betriebssystemausfällen:

- Wenn das Betriebssystem der virtuellen Maschine einen Fehler zurückgibt, kann die virtuelle Maschine automatisch auf derselben Hardware gestartet werden.
- Wenn die physische Hardware fehlerhaft ist, können die betroffenen virtuellen Maschinen automatisch auf anderen Servern im Cluster neu gestartet werden.

Mit vSphere HA können Sie Policies konfigurieren, um festzulegen, welche Maschinen unter welchen Bedingungen automatisch neu gestartet werden sollen.

VMware vShield Endpoint

Mit VMware vShield Endpoint können Sie Virenschutz- und Anti-Malware-Überprüfungsvorgänge an eine dedizierte sichere virtuelle Appliance auslagern, die von VMware-Partnern bereitgestellt wird. Die Auslagerung von Überprüfungsvorgängen verbessert die Desktopkonsolidierungsraten und -performance, indem Virenschutzspitzenlasten verhindert werden. Gleichzeitig werden Virenschutz- und Anti-Malware-Bereitstellung und -Monitoring rationalisiert und Compliance- und Auditanforderungen durch eine ausführliche Protokollierung der Virenschutz- und Anti-Malware-Aktivitäten erfüllt.

Rechnerebene

VSPEX definiert die Mindestanzahl der auf der Rechnerebene erforderlichen Ressourcen, ermöglicht dem Kunden jedoch, diese auf jeder beliebigen Serverhardware zu implementieren, die diese Anforderungen erfüllt. Weitere Informationen finden Sie unter Kapitel 5 dieses Leitfadens.

Netzwerkebene

VSPEX definiert die Mindestanzahl der für die Lösung erforderlichen Netzwerkports und stellt allgemeine Richtlinien zur Netzwerkarchitektur bereit, ermöglicht es dem Kunden jedoch, beliebige Netzwerkhardware zu verwenden, die diese Anforderungen erfüllt. Weitere Informationen finden Sie unter Kapitel 5 dieses Leitfadens.

Speicherebene

Die Speicherebene ist eine Schlüsselkomponente einer jeden Cloud-Infrastrukturlösung, die von Anwendungen und Betriebssystemen generierte Daten in ein System für die Rechenzentrum-Speicherverarbeitung einspeist. In dieser VSPEX-Lösung werden XtremIO-Speicherarrays für die Bereitstellung der Virtualisierung auf der Speicherebene verwendet. Die XtremIO-Plattform bietet die erforderliche Speicherperformance, erhöht die Speichereffizienz und Managementflexibilität und reduziert die Total Cost of Ownership. Diese Lösung verwendet zudem die Arrays der VNX-Produktreihe, um Speicher für Benutzerdaten zur Verfügung zu stellen.

EMC XtremIO

Das XtremIO-All-Flash-Array ist ein vollständig neues Design mit einer revolutionären Architektur. Es erfüllt alle erforderlichen Anforderungen, die das agile Rechenzentrum ermöglichen: lineares Scale-out, kontinuierliche Inline-Datenservices und umfangreiche Rechenzentrumsservices für die Workloads.

Der grundlegende Hardwarebaustein für diese Scale-out-Arrays ist der X-Brick-Baustein. Jeder X-Brick-Baustein hat zwei Aktiv-Aktiv-Controller-Nodes und ein Festplattenarraygehäuse zusammen in einem Paket. Der Starter-X-Brick-Baustein mit 13 SSDs kann ohne Ausfallzeit auf einen vollständigen X-Brick-Baustein mit 25 SSDs erweitert werden. Bis zu sechs X-Brick-Bausteine können in einem einzigen Scale-out-Cluster kombiniert werden, um die Performance und Kapazität linear zu erhöhen.

Die XtremIO-Plattform maximiert die Verwendung der Flash-Speichermedien. Hauptattribute dieser Plattform sind:

- Unglaublich hohe I/O-Performance, insbesondere für zufällige I/O-Workloads, die häufig in virtualisierten Umgebungen vorkommen
- Konsistent niedrige Latenz (unterhalb Millisekundenbereich)
- Echte Inline-Datenreduzierung: Entfernt redundante Informationen im Datenpfad und schreibt nur einmalige in das Array, wodurch die erforderliche Speicherkapazität gemindert wird
- Eine umfassende Suite von Enterprise-Arrayfunktionen, wie Integration in VMware über VAAI, N-Wege-Aktiv-Controller, hohe Verfügbarkeit, starker Datenschutz und Thin Provisioning

XtremIO-Speichersysteme enthalten die folgenden Komponenten:

- **Hostadapterports**: Bereitstellen einer Hostverbindung über eine Fabric in das Array
- **Speicher-Controller** (SCs): die Rechnerkomponente des Speicherarrays SCs werden für alle Aspekte der Datenverlagerung in, aus und zwischen Arrays eingesetzt

- **Festplattenlaufwerke**: Solid State Drives, die den Host und die Anwendungsdaten enthalten
- **InfiniBand-Switche**: ein Computernetzwerk-Datenübertragungslink in Multi-X-Brick-Bausteinkonfigurationen mit Switch, hohem Durchsatz, niedriger Latenz, Skalierbarkeit sowie Quality-of-Service- und Failover-Funktionalität

XtremIO Operating System (XIOS)

Das XtremIO-Betriebssystem (XIOS) verwaltet das XtremIO-Speichercluster. XIOS ermöglicht es, dass das System ausgeglichen bleibt. Es bietet auf folgende Weise die höchsten Performancelevel ohne Administratoreingriffe:

- Es wird ermöglicht, dass alle SSDs gleichmäßig belastet sind. Dadurch werden die höchstmögliche Performance und Belastbarkeit für anspruchsvolle Workloads erzielt.
- Die komplexe Konfiguration, die für herkömmliche Arrays erforderlich ist, wird eliminiert. Es besteht keine Notwendigkeit, RAID-Level festzulegen, Laufwerksgruppengrößen zu bestimmen, Stripe-Breiten und Caching-Policies festzulegen oder Aggregate zu erstellen.
- Konfiguriert jedes Volume jederzeit automatisch und optimal. I/O-Performance auf vorhandenen Volumes und Datensätzen erhöht sich automatisch bei großen Clustergrößen. Jedes Volume kann das vollständige Leistungspotenzial des gesamten XtremIO-Systems nutzen.

Standardbasiertes Enterprise-Speichersystem

Das XtremIO-System stellt eine Verbindung mit vSphere-Hosts über Standard-FC- und -iSCSI-Block-Schnittstellen her. Das System umfasst Funktionen für vollständige hohe Verfügbarkeit wie Support für natives VMware Multipath I/O, Schutz vor SSD-Ausfällen, unterbrechungsfreie Software- und Firmware-Upgrades, keinen Single Point of Failure (SPOF) und Hot-Swap-Komponenten.

Inlinedatenreduzierung in Echtzeit

Das XtremIO-Speichersystem dedupliziert und komprimiert Daten einschließlich Desktop-Images in Echtzeit, wodurch eine enorm hohe Anzahl virtueller Desktops mit wirtschaftlich geringem Aufwand bzgl. Flash-Speicher betrieben werden kann. Die Datenreduzierung auf dem XtremIO-Array wirkt sich nicht negativ auf die IOPS oder die Performance der Latenz aus; stattdessen wird die Performance der Anwender-Computing-Umgebung sogar gesteigert.

Scale-Out-Design

Der X-Brick ist der Grundbaustein eines Scale-out-XtremIO-Cluster-Systems. Durch Verwendung eines Starter-X-Brick-Bausteins kann die Bereitstellung virtueller Desktops in kleinem Maßstab beginnen und fast beliebig erweitert werden, indem sie bei Bedarf ein Upgrade für den Starter-X-Brick-Baustein auf einen X-Brick-Baustein durchführen und dann ein größeres XtremIO-Cluster konfigurieren, falls erforderlich. Das System erweitert die Kapazität und Performance linear, wenn Bausteine hinzugefügt werden. Dadurch werden die EUC-Dimensionierung und das Management künftigen Wachstums sehr einfach.

VAAI Integration

Das XtremIO-Array ist vollständig mit vSphere über vStorage APIs für Array-Integration (VAAI) integriert. Alle API-Befehle wie ATS, Clone Blocks/Full Copy/XCOPY, Zero Blocks/Write Same, Thin Provisioning und Block Delete werden unterstützt. Dies bietet in Kombination mit der Inline-Datenreduzierung des Arrays und dem In-Memory-Metadatenmanagement beinah sofortiges Provisioning und Klonen virtueller Maschinen und ermöglicht das Verwenden großer Volumes für einfaches Management.

Extreme Performance

Das XtremIO-Array verwaltet sehr hohe, konstante Mengen kleiner, zufälliger und gemischter I/O-Lese- und Schreibvorgänge, wie sie bei virtuellen Desktops üblicherweise vorkommen – und dies mit konsistenter, außergewöhnlich niedriger Latenz.

Schnelles Provisioning

XtremIO-Arrays verwenden beschreibbare Snapshot-Technologie, die speicherplatzeffizient für Daten und Metadaten ist. XtremIO-Snapshots sind frei von Begrenzungen der Performance, Funktionen, der Topologie oder der Kapazitätsreservierungen. Mit ihrer einmaligen Architektur der Metadaten im Arbeitsspeicher können XtremIO-Arrays Desktopumgebungen jeder Größe sofort klonen.

Anwenderfreundlichkeit

Das XtremIO-Speichersystem erfordert nur einige grundlegende Einrichtungsschritte und kein Tuning oder laufende Administration, um hohe Performance zu erreichen und zu erhalten. Das XtremIO-System kann in weniger als einer Stunde nach der Lieferung bereitgestellt werden.

Sicherheit mit Data-at-Rest-Verschlüsselung (D@RE)

XtremIO-Arrays verschlüsseln sicher alle Daten, die auf dem All-Flash-Array gespeichert sind, und bieten Schutz, insbesondere für Desktops mit vollständigen Clones, für regulierte Anwendungsbeispiele in sensiblen Branchen wie dem Gesundheitswesen, dem Finanzwesen und der Regierung.

Rechenzentrumsökonomie

Ein einziger X-Brick-Baustein kann Tausende von Desktops in einem Rack mit nur 6 HEs bei einem Strombedarf von ca. 750 W hosten.

EMC Isilon

Isilon Scale-out-NAS (Network Attached Storage) ist hervorragend für das Speichern großer Mengen von Benutzerdaten und Windows-Profilen in einer Horizon View-Infrastruktur geeignet. Er bietet eine einfache, skalierbare und effiziente Plattform zum Speichern enormer Mengen unstrukturierter Daten und ermöglicht verschiedenen Anwendungen die Erstellung eines skalierbaren und zugänglichen Daten-Repository ohne den Overhead, der bei herkömmlichen Speichersystemen entsteht. Hauptattribute der Isilon-Plattform sind:

- Isilon unterstützt mehrere Protokolle wie NFS, CIFS, HTTP, FTP, HDFS für Hadoop und Datenanalyse und REST für Objekt- und Cloud-Computing.
- Die Isilon-NAS-Architektur unterstützt in der Client-/Anwendungsschicht ein breites Spektrum von Betriebssystemumgebungen.

- Auf der Ethernetebene nutzt Isilon ein 10-GbE-Netzwerk.
- OneFS, das Betriebssystem von Isilon, ist eine Architektur mit einem einzigen Dateisystem und Volume, wodurch das Management unabhängig von der Anzahl der Nodes in Ihrem Isilon-Speichercluster erheblich vereinfacht wird.
- Isilon-Speichersysteme lassen sich von mindestens 3 Nodes auf bis zu 144 Nodes skalieren, die alle mit einer InfiniBand-Kommunikationsschicht verbunden sind.

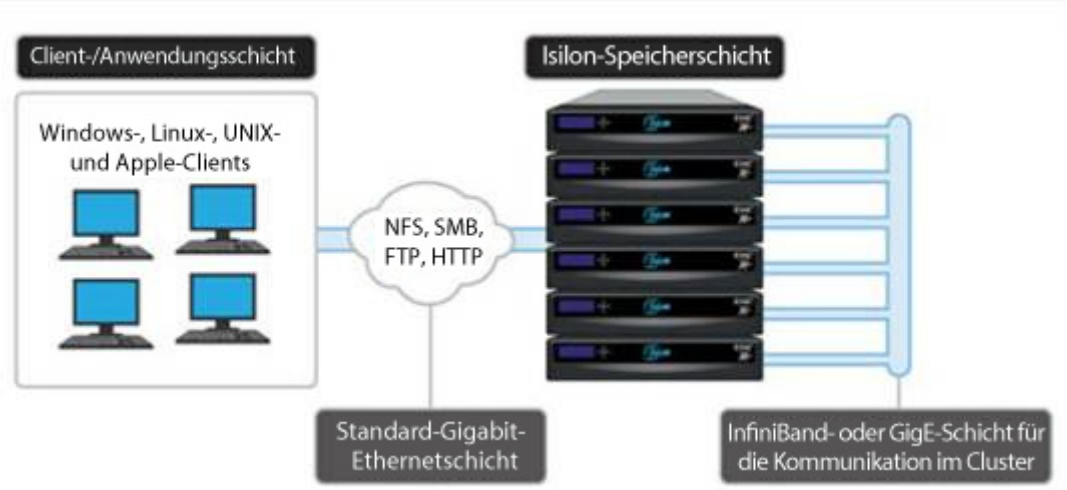


Abbildung 4. Isilon-Clusterkomponenten

Isilon OneFS

Das Isilon OneFS-Betriebssystem sorgt für die Intelligenz, die allen Isilon-Scale-out-Speichersystemen zugrunde liegt. Es werden die drei Schichten herkömmlicher Speicherarchitekturen – Dateisystem, Volume Manager und Datensicherheit – in einer einzigen Softwareschicht zusammengeführt und auf diese Weise ein einziges, intelligentes Dateisystem geschaffen, das alle Nodes in einem Isilon-Cluster umspannt.

Abbildung 5. Funktionen des Isilon OneFS-Betriebssystems

OneFS bietet eine Reihe wichtiger Vorteile:

- **Einfaches Management** in Folge des einzigen Dateisystems, einzigen Volume und des globalen Namespace der Isilon-Architektur
- **Enorme Skalierbarkeit** mit der Möglichkeit, auf 20 PB in einem einzigen Volume zu skalieren
- **Bisher unerreichte Effizienz** mit einer Speicherauslastung von über 80 %, automatisiertem Speicher-Tiering und Isilon SmartDedupe

- **Enterprise-Datensicherheit** einschließlich effizientem Backup und Disaster Recovery und N+1- bis N+4-Redundanz
- **Robuste Sicherheits- und Compliance-Optionen** mit:
  - Rollenbasierte Zugriffskontrolle
  - Sichere Zugriffszonen
  - SEC 17a-4-vorgabenkonforme WORM-Datensicherheit
  - Data-at-Rest-Verschlüsselung (DARE) mit Self-Encrypting-Drives (SED)
  - Integrierte Unterstützung für Dateisystemauditing
- **Betriebliche Flexibilität** mit Multiprotokollunterstützung einschließlich nativem HDFS-Support; Syncplicity®-Support für sicheres mobiles Computing und Support für Objekt- und Cloud-Computing einschließlich OpenStack Swift

Isilon bietet Ihnen eine vollständige Datensicherheits- und Managementsoftware, die Ihnen den Schutz Ihrer Datenressourcen, die Kontrolle Ihrer Kosten und die Optimierung Ihrer Speicherressourcen und Systemperformance für Ihre Big Data-Umgebung erleichtert.

Datenschutz

- **SnapshotIQ**: Effizienter und zuverlässiger Schutz für Daten mit sicheren, nahezu sofortigen Snapshots bei geringem oder gar keinem Performance-Overhead und schnellere Recovery wichtiger Daten mit nahezu sofortigen Snapshot-Wiederherstellungen nach Bedarf
- **SyncIQ**: Replikation und Verteilung großer, geschäftskritischer Datenmengen zur Multiplizierung freigegebener Speichersysteme an mehreren Standorten für die Fähigkeit einer zuverlässigen Disaster Recovery
- **SmartConnect**: Ermöglicht einen Lastenausgleich für Clientverbindungen und ein dynamisches NFS-Failover und -Failback von Clientverbindungen zwischen Speicher-Nodes zur Optimierung der Nutzung von Clusterressourcen
- **SmartLock**: Schutz Ihrer wichtigen Daten vor versehentlichem, vorzeitigem oder böswilligem Ändern oder Löschen mit unserem softwarebasierten WORM-Ansatz (Write Once Read Many) und Einhaltung strenger Compliance- und Governance-Anforderungen wie SEC 17a-4

Datenmanagement

- **SmartPools:** Implementiert eine hocheffiziente, automatisierte Tiered-Storage-Strategie zur Optimierung der Speicherperformance und -kosten
- **SmartDedupe:** Datendeduplizierung zur Reduzierung von Speicherkapazitätsanforderungen und der zugehörigen Kosten ohne Performanceeinbußen
- **SmartQuotas:** Managt und weist Quotas zu für eine nahtlose Partitionierung und Thin Provisioning von Speicher in einfach zu managende Segmente auf Cluster-, Verzeichnis-, Unterverzeichnis-, Benutzer- und Gruppenebene
- **InsightIQ:** Zusätzliche innovative Tools für das Performancemonitoring und Reporting, die Ihnen die Maximierung der Performance Ihres Isilon Scale-out-Speichersystems erleichtern können
- **Isilon für vCenter:** Management von Isilon-Speicherfunktionen im vCenter

Isilon Scale-out-NAS-Produktreihe

Die heute verfügbaren Isilon-Nodes sind entsprechend ihrer Funktion in eine Reihe von Klassen unterteilt:

- **S-Serie**: IOPS-intensive Anwendungen
- **X-Serie**: Workflows mit vielen gleichzeitigen Zugriffen und hohem Durchsatz
- **NL-Serie**: Nahezu Primärspeichern entsprechende Zugriffszeiten zu vergleichbaren Kosten wie beim Einsatz von Bandsystemen
- **Performance-Accelerator**: Unabhängige Skalierung für maximale Performance
- **Backup-Accelerator**: Skalierbare Hochgeschwindigkeitslösung für das Backup und die Wiederherstellung von Daten

Abbildung 6. Isilon-Node-Klassen

EMC VNX

Die Flash-optimierte Unified Storage-Plattform VNX ist für die Speicherung von Benutzerdaten und Windows-Profilen in einer VMware Horizon View-Infrastruktur geeignet und stellt Innovationen und Funktionen der Enterprise-Klasse für Datei-, Block- und Objektspeicher in einer einzigen skalierbaren und anwenderfreundlichen Lösung bereit. VNX ist ideal für gemischte Workloads in physischen oder virtuellen Umgebungen geeignet und kombiniert leistungsstarke und flexible Hardware mit fortschrittlicher Software für Effizienz, Management und Schutz. So erfüllt es die anspruchsvollen Anforderungen der heutigen virtualisierten Anwendungsumgebungen.

VNX-Speichersysteme enthalten die folgenden Komponenten:

- **Hostadapterports** (für Block): Bereitstellung von Hostkonnektivität über eine Fabric in das Array.
- **Data Mover** (für File-basierten Speicher): Front-end-Appliances, die Dateiservices für Hosts bereitstellen (optional, wenn CIFS/SMB- oder NFS-Services bereitgestellt werden)
- **Speicherprozessoren** (SPs): die Rechnerkomponente des Speicherarrays. SPs werden für alle Aspekte der Datenverlagerung in, aus und zwischen Arrays eingesetzt.
- **Festplattenlaufwerke**: Festplattenspindeln und Solid-State-Laufwerke (SSDs) mit den Host-/Anwendungsdaten sowie zugehörige Gehäuse

Hinweis: Der Begriff Data Mover bezieht sich auf eine VNX-Hardwarekomponente, die über eine CPU, Arbeitsspeicher und I/O-Ports (Eingabe/Ausgabe) verfügt. Sie ermöglicht CIFS- (SMB-) und NFS-Protokolle auf dem VNX-Array.

EMC VNX-Serie

VNX umfasst viele Funktionen und Verbesserungen, die auf dem Erfolg der ersten Generation aufbauen, z. B.:

- Mehr Kapazität und bessere Optimierung mit VNX MCx™-Technologiekomponenten, darunter Multicore Cache, Multicore RAID und Multicore FAST Cache
- Höhere Effizienz mit einem Flash-optimierten Hybridarray
- Besserer Schutz durch die Erhöhung der Anwendungsverfügbarkeit mithilfe von Aktiv-Aktiv-Speicherprozessoren
- Einfachere Verwaltung und Bereitstellung mit der neuen Unisphere® Management Suite

VSPEX ist mit VNX dafür ausgelegt, noch mehr Effizienz, Performance und Skalierbarkeit als bisher zu bieten.

Flashoptimiertes Hybridarray

VNX ist ein flashoptimiertes Hybridarray, das dank automatisiertem Tiering eine optimale Performance für Ihre geschäftskritischen Daten ermöglicht und gleichzeitig weniger häufig genutzte Daten intelligent auf kostengünstigere Festplattenlaufwerke auslagert.

Bei diesem hybriden Ansatz kann ein geringer Prozentsatz der Flashlaufwerke im gesamten System einen hohen Prozentsatz der gesamten IOPS bereitstellen. Mit der Flashoptimierung macht VNX sich die geringe Latenz von Flash optimal zunutze, um kostensparende Optimierung und hochleistungsfähige Skalierbarkeit bereitzustellen. Die EMC Fully Automated Storage Tiering Suite (FAST Cache und FAST VP) verteilt sowohl block- als auch dateibasierte Daten auf verschiedene Speicherebenen auf heterogenen Laufwerken und stuft die aktivsten Daten in die Flashlaufwerke hoch, damit der Anwender in Bezug auf Kosten oder Performance keine Kompromisse eingehen muss.

In der Regel werden Daten zum Zeitpunkt ihrer Erstellung am häufigsten verwendet. Daher werden neue Daten für die beste Performance zunächst in Flashlaufwerken gespeichert. Werden die Daten älter und im Laufe der Zeit weniger aktiv genutzt, verschiebt FAST VP auf Basis von kundenspezifischen Richtlinien die Daten von Laufwerken mit hoher Performance automatisch auf Laufwerke mit hoher Kapazität. Diese Funktionen wurden mit einer viermal besseren Granularität und mit neuen FAST VP-SSDs (Solid State Disks) basierend auf eMLC-Technologie (Enterprise Multilevel Cell) verbessert, sodass die Kosten pro Gigabyte gesunken sind.

FAST Cache nutzt Flashlaufwerke als erweiterte Cacheebene, damit das Array dynamisch unvorhergesehene Spitzen bei den System-Workloads ausgleichen kann. Häufig aufgerufene Daten werden in 64-KB-Blöcken in den FAST Cache kopiert und nachfolgende Lese- oder Schreibzugriffe auf den Datenblock werden von FAST Cache verarbeitet. Dies ermöglicht das sofortige Verschieben sehr aktiver Daten auf Flashlaufwerke, wodurch die Antwortzeiten der aktiven Daten deutlich verbessert und Probleme beim Datenzugriff innerhalb der LUN verringert werden können.

Alle VSPEX-Anwendungsbeispiele profitieren von dieser gesteigerten Effizienz, die von der FAST Suite bereitgestellt wird. Weiterhin bietet VNX blockbasierte Out-of-Band-Deduplizierung, mit der sich die Kosten für die Flash-Tier-Kosten erheblich reduzieren lassen.

Unisphere Management Suite

EMC Unisphere® ist die zentrale Managementplattform für die VNX-Serie und enthält eine einzige kombinierte Ansicht der File- und Blocksysteme mit allen Funktionen, die über eine gemeinsame Benutzeroberfläche verfügbar sind. Unisphere ist für virtuelle Anwendungen optimiert und bietet eine branchenführende VMware-Integration. Virtuelle Maschinen und ESX-Server werden automatisch erkannt und es erfolgt eine End-to-End-Zuweisung für virtuelle und physische Ressourcen. Unisphere vereinfacht außerdem die Konfiguration von FAST Cache und FAST VP auf VNX-Plattformen.

Bei der neuen Unisphere Management Suite wurde die benutzerfreundliche Oberfläche von Unisphere um VNX Monitoring and Reporting erweitert, um die Performance überwachen und Kapazitätsanforderungen frühzeitig vorhersehen zu können. Wie in Abbildung 7 gezeigt, enthält die Suite außerdem Unisphere Remote für das zentrale Management von Tausenden von VNX- und VNXe-Systemen und bietet zusätzlich Support für XtremSW Cache.

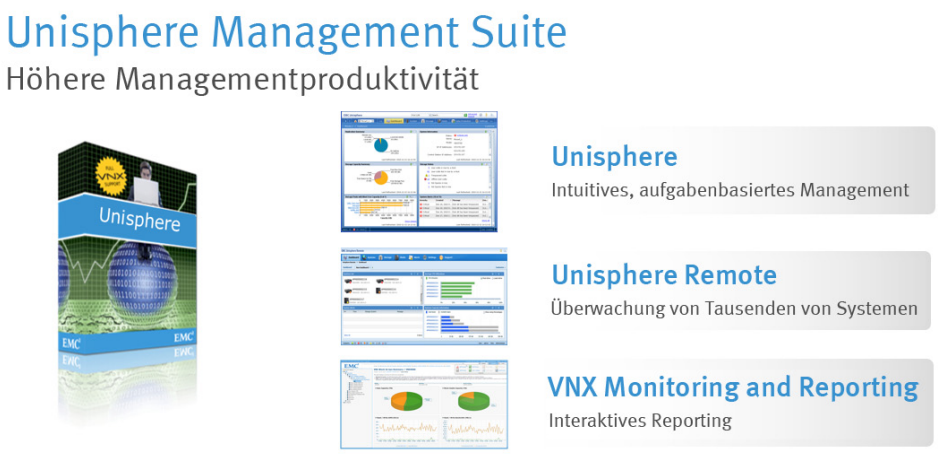


Abbildung 7. Neue Unisphere Management Suite

VMware Storage APIs for Storage Awareness

VMware vSphere Storage API for Storage Awareness (VASA) ist eine VMware-definierte API zum Anzeigen von Speicherinformationen über vCenter. Aufgrund der Integration zwischen VASA-Technologie und der VNX wird das Speichermanagement in einer virtualisierten Umgebung zu einer nahtlosen Erfahrung.

EMC VNX Virtual Provisioning

EMC VNX Virtual Provisioning™ ermöglicht Unternehmen die Reduzierung der Speicherkosten durch die Steigerung der Kapazitätsauslastung, Vereinfachung des Speichermanagements und Reduzierung der Ausfallzeiten von Anwendungen. Darüber hinaus hilft Virtual Provisioning Kunden, den Strom- und Kühlungsbedarf zu reduzieren und Investitionsausgaben zu senken.

Virtual Provisioning bietet poolbasiertes Speicher-Provisioning durch Implementieren von Pool-LUNs, die entweder „Thin“ oder „Thick“ sein können. Thin-LUNs bieten Speicher nach Bedarf, der die Auslastung Ihres Speichers maximiert, indem Speicher nur dort zugewiesen wird, wo er benötigt wird. Thick-LUNs bieten hohe und zuverlässige Performance für Ihre Anwendungen. Beide Arten von LUNs profitieren von den benutzerfreundlichen poolbasierten Provisioning-Funktionen.

Pools und Pool-LUNs sind die Bausteine für erweiterte Datenservices wie FAST VP, VNX-Snapshots und Komprimierung. Pool-LUNs unterstützen außerdem verschiedene zusätzliche Funktionen wie LUN-Verkleinerung, Onlineerweiterung und Einstellung des Schwellenwerts für die Benutzerkapazität.

VNX-Dateifreigaben

In vielen Umgebungen ist es wichtig, einen gemeinsamen Speicherort für Dateien zu besitzen, auf die viele Benutzer zugreifen. Diese Funktionalität wird in Form von CIFS- oder NFS-Dateifreigaben von einem Dateiserver implementiert. Die VNX-Speicherarrays können diesen Service zusammen mit dem zentralen Management, der Clientintegration, erweiterten Sicherheitsoptionen und Funktionen zur Verbesserung der Effizienz bereitstellen. Weitere Informationen zu VNX-Dateifreigaben finden Sie in folgendem Dokument: *EMC VNX-Serie: Konfiguration und Management von CIFS auf VNX* auf der EMC Online Support-Website.

EMC SnapSure

EMC SnapSure™ ist eine Softwarefunktion von VNX File, mit der Sie Kontrollpunkte erstellen und managen können, die logische Point-in-Time-Images eines PFS (Production File System) darstellen. SnapSure verwendet ein Copy-On-First-Modify-Prinzip. Ein PFS besteht aus Blöcken; wenn ein Block innerhalb eines PFS verändert wird, wird eine Kopie mit dem Originalinhalt des Blocks in einem separaten Volume namens SavVol gespeichert.

Nachfolgende Änderungen, die am selben Block im PFS vorgenommen werden, werden nicht im SavVol gespeichert. Die Originalblocks aus dem PFS im SavVol und die verbleibenden unveränderten PFS-Blöcke im PFS werden von SnapSure entsprechend einer Bitmap- und Blockmap-Datennachverfolgungsstruktur gelesen. Diese Blöcke werden zusammengefasst, um ein vollständiges Point-in-Time-Image bereitzustellen, das als „Kontrollpunkt“ bezeichnet wird.

Ein Kontrollpunkt spiegelt den Zustand eines PFS zum Zeitpunkt der Erstellung des Kontrollpunkts wider. SnapSure unterstützt folgenden Kontrollpunkte:

- Schreibgeschützte Kontrollpunkte: schreibgeschützte Dateisysteme, die aus einem PFS erstellt werden
- Beschreibbare Kontrollpunkte: beschreibbare Dateisysteme, die aus einem schreibgeschützten Kontrollpunkt erstellt werden

SnapSure kann maximal 96 schreibgeschützte Kontrollpunkte und 16 schreibfähige Kontrollpunkte pro PFS unterstützen, während PFS-Anwendungen weiterhin Zugriff auf Echtzeitdaten erhalten.

Hinweis: Jeder schreibfähige Kontrollpunkt ist einem schreibgeschützten Kontrollpunkt zugeordnet, der als Basiskontrollpunkt bezeichnet wird. Jeder Basiskontrollpunkt kann nur einen zugehörigen schreibfähigen Kontrollpunkt haben.

Weitere Informationen finden Sie in *Verwenden von VNX SnapSure*.

Virtualisierungs-management

VMware Virtual Storage Integrator (VSI) für VMware vSphere Web Client

Der VMware Virtual Storage Integrator (VSI) für VMware vSphere-Webclient ist ein Plug-in für VMware vCenter. Er ermöglicht Administratoren das Anzeigen, Managen und Optimieren von Speicher für VMware ESX/ESXi-Server und Hosts und das anschließende Zuweisen von Speicher zu den Hosts.

VSI besteht aus einer grafischen Benutzeroberfläche und dem EMC Solutions Integration Service (SIS), der die Kommunikation mit den Speichersystemen und den Zugriff auf sie ermöglicht. Je nach der Plattform können Sie beispielsweise folgende Aufgaben mit VSI ausführen:

- Speicher-Provisioning
- Cloning
- Blockdeduplizierung
- Compression
- Speicherzuordnung
- Kapazitätsüberwachung
- Integration der Virtual Desktop Infrastructure (VDI)

Mit der Speicherzugriffsfunktion kann ein Speicheradministrator virtuellen Administratoren das Ausführen von Managementaufgaben auf einem Satz Speicherpools ermöglichen.

Die aktuelle Version von VSI unterstützt die folgenden EMC Speichersysteme und Funktionen:

- EMC ViPR™ Software Defined Storage
  - Anzeigen der Eigenschaften von NFS- und VMFS-Datenspeichern und RDM-Volumes
  - Provisioning von NFS- und VMFS-Datenspeichern und RDM-Volumes
- VNX-Speicher für ESX/ESXi-Hosts
  - Anzeigen der Eigenschaften von NFS- und VMFS-Datenspeichern und RDM-Volumes
  - Provisioning von NFS- und VMFS-Datenspeichern und RDM-Volumes
  - Komprimieren und Dekomprimieren von Speichersystemobjekten auf NFS- und VMFS-Datenspeichern
  - Aktivieren und Deaktivieren der Blockdeduplizierung auf VMFS-Datenspeichern
  - Erstellen von schnellen oder vollständigen Clones von virtuellen Maschinen für NFS-Dateispeicher
- EMC Symmetrix® VMAX®-Speichersysteme
  - Anzeigen der Eigenschaften von VMFS-Datenspeichern und RDM-Volumes
  - Provisioning von VMFS-Datenspeichern und RDM-Volumes
- XtremIO-Speichersysteme
  - Anzeigen der Eigenschaften von ESX/ESXi-Datenspeichern und RDM-Festplatten

- Provisioning von VMFS-Datenspeichern und RDM-Volumes
- Erstellen vollständiger Clones mit XtremIO-nativen Snapshots
- Integration in VMware Horizon View und Citrix XenDesktop

Weitere Informationen finden Sie in den Produktleitfäden zu EMC VSI für VMware vSphere auf der EMC Online Support-Website.

Datensicherheitsebene

Avamar bietet den erforderlichen Schutz, um die Bereitstellung von VSPEX-Lösungen für Anwender-Computing zu beschleunigen.

Mit Avamar können Administratoren Policies und Komponenten der Anwender-Computing-Infrastruktur zentral sichern und managen, während Anwender gleichzeitig auf effiziente Weise eigene Dateien über eine einfache und intuitive webbasierte Benutzeroberfläche wiederherstellen können. Da nur neue und eindeutige Datensegmente der Subdatei verschoben werden, ermöglicht Avamar schnelle tägliche komplette Backups mit einer um bis zu 90 % kürzeren Backup-Zeit und reduziert gleichzeitig die erforderliche tägliche Netzwerkbandbreite um bis zu 99 %. Alle Recoveries mit Avamar werden in einem einzigen Schritt ausgeführt.

Weitere Informationen finden Sie im *EMC Backup und Recovery für VSPEX für Anwender-Computing mit VMware Horizon View – Design- und Implementierungsleitfaden*.

Sicherheitsschicht

Die Zwei-Faktor-Authentifizierung von RSA SecurID sorgt für zusätzliche Sicherheit für die VSPEX Anwender-Computing-Umgebung, da der Benutzer sich mit zwei Arten von Daten authentifizieren muss. Diese Daten werden als Passphrase bezeichnet. Die SecurID-Funktion wird über den RSA Authentication Manager verwaltet, der zudem für Verwaltungsfunktionen wie die Zuordnung von Tokens zu Benutzern, Benutzermanagement und Hochverfügbarkeit zuständig ist.

Der *Designleitfaden Sicherung des EMC VSPEX-Anwender-Computing mit RSA SecurID: VMware Horizon View 5.2 und VMware vSphere 5.1 für bis zu 2.000 virtuelle Desktops* stellt Details für die Planung der Sicherheitsebene bereit.

VMware Workspace-Lösung

VMware Workspace kombiniert Anwendungen in einer einzigen, integrierten Arbeitsumgebung und bietet Mitarbeitern die Flexibilität, auf die Arbeitsumgebung auf jedem Gerät zugreifen zu können, unabhängig davon, wo sie sich gerade befinden. VMware Workspace reduziert die Komplexität der Administration, indem es der IT ermöglicht, diese Ressourcen über alle Geräte hinweg zentral bereitzustellen, zu managen und zu sichern.

Mit einigen Infrastrukturergänzungen unterstützt die VSPEX-Lösung für Anwender-Computing für VMware Horizon View auch VMware Workspace-Bereitstellungen.

Kapitel 4 Dimensionierung der Lösung

In diesem Kapitel werden die folgenden Themen behandelt:

Übersicht 40

Referenz-Workload 40

VSPEX Private Cloud-Anforderungen: 41

XtremIO-Arraykonfigurationen 42

Isilon-Konfiguration 43

VNX-Konfigurationen 44

Auswählen der geeigneten Referenzarchitektur 45

Übersicht

In diesem Kapitel wird beschrieben, wie Sie eine VSPEX-Lösung für Anwender-Computing für VMware Horizon View entwerfen und gemäß den Anforderungen eines Kunden dimensionieren. Es werden die Konzepte eines Referenz-Workload, Bausteine sowie die validierten Maximalwerte für das Anwender-Computing vorgestellt und gezeigt, wie Sie damit Ihre Lösung entwerfen können. In Tabelle 4 zeigt die allgemeinen Schritte, die Sie bei der Dimensionierung der Lösung ausführen müssen.

Tabelle 4. VSPEX Anwender-Computing: Designprozess

Schritt	Aktion
1	Verwenden Sie das Arbeitsblatt für die Kundenkonfiguration in Anhang A, um die Kundenanforderungen für die Anwender-Computing-Umgebung zu erfassen.
2	Verwenden Sie das EMC VSPEX-Dimensionierungstool, um die empfohlene VSPEX-Referenzarchitektur für Ihre Anwender-Computing-Lösung auf Basis der in Schritt 1 erfassten Kundenanforderungen zu ermitteln. **Hinweis:** Sollte das Dimensionierungstool nicht zur Verfügung stehen, können Sie die Anwender-Computing-Lösung manuell mithilfe der Richtlinien in diesem Kapitel dimensionieren.

Referenz-Workload

VSPEX definiert einen Referenz-Workload, der eine Maßeinheit für die Quantifizierung der Ressourcen in den Referenzarchitekturen der Lösung darstellt. Durch den Vergleich der tatsächlichen Auslastung des Kunden mit diesem Referenz-Workload können Sie ableiten, welche Referenzarchitektur Sie als Basis für die VSPEX-Bereitstellung des Kunden auswählen sollten.

Für VSPEX-Lösungen für Anwender-Computing ist der Referenz-Workload ein einziger virtueller Desktop – der virtuelle Referenzdesktop –, der die in Tabelle 5 aufgeführten Workload-Merkmale aufweist.

Um die entsprechende Anzahl der virtuellen Desktops für eine bestimmte Ressourcenanforderung zu bestimmen, verwenden Sie das VSPEX-Arbeitsblatt für die Kundenkonfiguration um die tatsächlichen Gesamtressourcen zu konvertieren, die für alle Desktops in das Format des virtuellen Desktops erforderlich sind.

Tabelle 5. Merkmale der virtuellen Referenzmaschine

Eigenschaft	Wert
Betriebssystem der virtuellen Desktops	Microsoft Windows 7 Enterprise Edition (32-Bit) oder Microsoft Windows 8.1 Enterprise Edition (32-Bit)
Virtuelle Prozessoren pro virtuellen Desktop	1
RAM pro virtuellen Desktop	2 GB
Durchschnittliche IOPS pro virtuellem Desktop in stationärem Zustand	10
Internet Explorer	10 für Windows 7 oder 11 für Windows 8.1

Eigenschaft	Wert
standort	2010
Adobe Reader	XI
Adobe Flash Player	11 ActiveX
Doro PDF-Drucker	1,8
Workload-Generator	Login VSI 4.1.2
Workload-Typ	Büromitarbeiter

Diese Desktopdefinition basiert auf Benutzerdaten, die sich im gemeinsamen Speicher befinden. Das I/O-Profil wird mithilfe eines Test-Framework definiert, in dem alle Desktops gleichzeitig mit einer gleichmäßigen Last ausgeführt werden, die von der konstanten Verwendung bürobasierter Anwendungen wie Browsern und Büroproduktivitäts-Suites erzeugt wird.

Diese Lösung ist mit Performancetests verifiziert, die mithilfe von Login VSI (*www.loginvsi.com*) durchgeführt wurden, der Belastungstestlösung nach Branchenstandard für virtualisierte Desktopumgebungen.

Login VSI bietet proaktive Performancemanagementlösungen für virtualisierte Desktop- und Serverumgebungen. Unternehmens-IT-Abteilungen verwenden Login VSI-Produkte in allen Phasen ihrer Bereitstellung virtueller Desktops, von der Planung über die Bereitstellung bis zum Änderungsmanagement, für eine zuverlässigere Performance, höhere Verfügbarkeit und eine konsistentere Anwendererfahrung. Die weltweit führenden Anbieter von Virtualisierung verwenden das Vorzeigeprodukt, Login VSI, zum Benchmarking von Performance. Mit nur minimaler Konfiguration funktionieren Login VSI-Produkte in VMware Horizon View, Citrix XenDesktop und XenApp, Microsoft Remote Desktop Services (Terminal Services) und jeder anderen Windows-basierten virtuellen Desktoplösung.

Laden Sie für weitere Informationen eine Testversion unter *www.loginvsi.com* herunter.

VSPEX Private Cloud-Anforderungen:

Diese VSPEX-Anwender-Computing Proven Infrastructure erfordert mehrere Anwendungsserver. Sofern nicht anders angegeben, verwenden alle Server Microsoft Windows Server 2012 R2 als das Basisbetriebssystem. In Tabelle 6 listet die Mindestanforderungen für die einzelnen erforderlichen Infrastrukturserver auf.

Tabelle 6. Mindestanforderungen für den Infrastrukturserver

Server	CPU	RAM	IOPS	Speicherkapazität
Domain-Controller (je)	2 vCPUs	4 GB	25	32 GB
SQL Server	2 vCPUs	6 GB	100	200 GB
vCenter Server	4 vCPUs	8 GB	100	80 GB
View-Controller (je)	4 vCPUs	12 GB	50	32 GB

Die Anforderungen für den optionalen VMware vRealize Operations Manager für Horizon View- und VMware Workspace-Komponenten sind in den folgenden Abschnitten dieses Dokuments verfügbar:

- VMware vRealize Operations Manager für Horizon View – Plattformprofil
- VSPEX-Lösung für VMware Workspace

Speicherlayout der Private Cloud

Diese Lösung benötigt die folgenden Volumes der angezeigten Größe für das Speichern der angegebenen virtuellen Maschinen:

- Ein 1-TB-Volume, um die virtuelle Maschinen des Infrastrukturserver zu hosten, die den VMware vCenter Server, die View Connection Server, die Microsoft Active Directory-Server und die Microsoft SQL Server enthalten können.
- Für Konfigurationen für bis zu 1.750 Desktops: ein 1,8-TB-Volume, um den vRealize Operations Manager für virtuelle Maschinen und Datenbanken mit Horizon View zu hosten
- Für Konfigurationen für bis zu 3.500 Desktops: ein 3,6-TB-Volume, um den vRealize Operations Manager für virtuelle Maschinen und Datenbanken mit Horizon View zu hosten

Weitere Informationen über größere Konfigurationen erhalten Sie von Ihrem EMC Vertriebsmitarbeiter.

XtremIO-Arraykonfigurationen

Wir validierten die VSPEX XtremIO-Konfigurationen für Anwender-Computing auf den Starter-X-Brick- und X-Brick-Plattformen, die sich gemäß der Anzahl von SSDs und ihrer verfügbare Gesamtkapazität unterscheiden. Für jedes Array empfiehlt EMC eine maximale VSPEX-Konfiguration für Anwender-Computing, wie in diesem Abschnitt erläutert.

Validierte XtremIO-Konfigurationen

Die folgenden XtremIO-validierten Laufwerkslayouts wurden erstellt, um die angegebene Anzahl virtueller Desktops mit einem definierten Performancelevel zu unterstützen. Diese VSPEX-Lösung unterstützt 2 XtremIO-X-Brick-Bausteinkonfigurationen, die auf Basis der Anzahl der bereitgestellten Desktops ausgewählt werden.

- XtremIO-Starter-X-Brick-Baustein: unterstützt virtuelle Desktops mit bis zu 1.250 vollständigen Clones oder 1.750 verknüpften Clones
- XtremIO-X-Brick-Baustein: unterstützt virtuelle Desktops mit bis zu 2.500 vollständigen Clones oder 3.500 verknüpften Clones

Die für diese Lösung erforderliche XtremIO-Storage-Konfiguration gilt zusätzlich zum Speicher, der von der VSPEX Private Cloud benötigt wird, welche die Infrastrukturservices der Lösung unterstützt. Weitere Informationen über den VSPEX Private-Cloud-Speicherpool finden Sie im VSPEX Proven Infrastructure-Leitfaden in Grundlegende Dokumente.

XtremIO-Speicherlayout

In Tabelle 7 zeigt die Anzahl der XtremIO-Volumes, die die Lösung den vSphere-Servern als VMFS-Datastores für virtuellen Desktopspeicher präsentiert.

Tabelle 7. XtremIO-X-Brick-Konfigurationen

XtremIO-Konfiguration	Anzahl der Desktops	Desktoptyp	Anzahl Volumes	Größe des Volumes
Starter-X-Brick	1.250	vollständige Clones	10	5 TB
	1.750	verknüpfte Clones	14	1 TB
X-Brick	2.500	vollständige Clones	20	5 TB
	3.500	verknüpfte Clones	28	1 TB

Erweitern vorhandener VSPEX-Anwender-Computing-Umgebungen

Die EMC VSPEX-Lösung für Anwender-Computing basiert auf einem flexiblen Implementierungsmodell, das eine einfache Erweiterung der Umgebung bei Bedarf ermöglicht.

Um zukünftige Erweiterungen zu unterstützen, kann der XtremIO-Starter-X-Brick unterbrechungsfrei zu einem X-Brick erweitert werden, indem die XtremIO-Erweiterungsausrüstung installiert wird, welche zusätzlich zwölf 400 GB-SSD-Laufwerke hinzufügt. Ein Starter-X-Brick-Baustein, der auf diese Weise erweitert wurde, unterstützt virtuelle Desktops mit bis zu 2.500 vollständigen Clones oder 3.500 verknüpften Clones.

Um virtuelle Desktops mit mehr als 3.500 verknüpften Clones oder mehr als 2.500 vollständigen Clones zu unterstützen, unterstützt XtremIO ein Online-Scale-out durch Hinzufügen weiterer X-Brick-Bausteine. Jeder zusätzliche X-Brick erhöht die Performance und virtuelle Desktopkapazität linear. XtremIO-Cluster mit zwei X-Bricks, vier X-Bricks oder sechs X-Bricks sind gültige Konfigurationen.

Isilon-Konfiguration

Diese Lösung verwendet das Isilon-System zum Speichern von Benutzerdaten, Home-Verzeichnissen und Profilen. Ein Isilon-Cluster mit drei Nodes unterstützt die Daten von 2.500 Benutzern mit dem Referenz-Workload, der in dieser Lösung validiert wurde. Jeder Node hat 36 Laufwerke (2 EFD und 34 SATA) und zwei 10-GbE-Ports. Tabelle 8 enthält detaillierte Informationen:

Tabelle 8. Ressourcenanforderungen für Benutzerdaten auf Isilon

Anzahl der virtuellen Referenz-Desktops	Isilon-Konfiguration		Max. Kapazität/Benutzer (GB)
	Node-Nummer.	Node-Typ	
1 ~ 2.500	3	X410	36
2.501,3.500	4	X410	35
3.501,5.000	5	X410	30

In Tabelle 8 ist eine Empfehlung für eine Isilon-Konfiguration mit der Anzahl der CIFS-Aufrufe als Erfüllungs-Baseline dargestellt. Jeder X410-Node, der in dieser Lösung verwendet wird, kann 30 TB Kapazität bereitstellen. Fügen Sie mehr Nodes hinzu, wenn mehr Kapazität pro Benutzer benötigt wird.

Diese Lösung kann auch andere Isilon-Node-Typen unterstützen. Weitere Informationen erhalten Sie im VSPEX-Dimensionierungstool oder von Ihrem EMC Vertriebsmitarbeiter.

VNX-Konfigurationen

Diese Lösung unterstützt auch die Verwendung von Speicherarrays der VNX-Serie für die Speicherung von Benutzerdaten mit aktiviertem FAST-Cache für die dazugehörigen Speicherpools. Die VNX5400™ kann bis zu 1.750 ´Benutzer mit dem in dieser Lösung validierten Referenz-Workload unterstützen. Die VNX5600™ kann bis zu 3.500 Benutzer mit demselben Referenz-Workload unterstützen. In Tabelle 9 sind die detaillierten Anforderungen für 1.250 – 3.500 Benutzer dargestellt.

Tabelle 9. Ressourcenanforderung für Benutzerdaten auf VNX

Anzahl der Benutzer	VNX-Modell	SSD für FAST-Cache	Anzahl der NL-SAS-Laufwerke mit je 2 TB	Max. Kapazität/ Benutzer (GB)
1.250	5400	2	16	15
1.750	5400	2	32	22
2.500	5600	4	40	19
3.500	5600	4	48	17

In Tabelle 9 ist eine Empfehlung für eine VNX-Konfiguration mit der Anzahl der CIFS-Aufrufe als Erfüllungs-Baseline dargestellt. Jede in dieser Lösung verwendete RAID-6-Gruppe mit 6+2 NL-SAS mit jeweils 2 TB kann 10 TB Kapazität bereitstellen. Fügen Sie weitere RAID-6-Gruppen mit 6+2 NL-SAS mit jeweils 2 TB hinzu, wenn mehr Kapazität pro Benutzer benötigt wird.

Weitere Informationen zu umfangreicheren Anforderungen erhalten Sie im VSPEX-Dimensionierungstool oder von Ihrem EMC Vertriebsmitarbeiter.

VNX FAST VP

Wenn mehrere Laufwerkstypen implementiert sind, aktivieren Sie FAST VP, um ein automatisches Daten-Tiering zu erreichen und die Unterschiede in Performance und Kapazität auszugleichen.

Hinweis: FAST VP kann zu einer Verbesserung der Performance führen, wenn es für Benutzerdaten und Roaming-Profile implementiert wird. Verwenden Sie FAST VP nicht für virtuelle Desktop-Datastores.

Gemeinsame VNX-Dateisysteme

In dieser validierten Lösung verwenden die virtuellen Desktops vier gemeinsame Dateisysteme – zwei für die VMware View Horizon Persona Management Repositories und zwei für die Umleitung von Benutzerspeicher, der sich in Stammverzeichnissen befindet. Im Allgemeinen ermöglicht die Umleitung von Benutzerdaten aus dem Basis-Image auf Isilon oder VNX die Zentralisierung von Administration und Datensicherheit und erhöht die Zustandslosigkeit („stateless“) der Desktops. Jedes Dateisystem wird über eine CIFS-Share in die Umgebung exportiert. Jede Persona Management Repository-Share und jede Stammverzeichnis-Share bedient die gleiche Anzahl von Benutzern.

Auswählen der geeigneten Referenzarchitektur

Wenn Sie die passende Referenzarchitektur für eine Kundenumgebung auswählen, müssen Sie die Ressourcenanforderungen der Umgebung bestimmen und diese Anforderungen dann in eine entsprechende Anzahl virtueller Referenzdesktops umrechnen, die die in Tabelle 5 auf Seite 40 aufgeführten Merkmale aufweisen. In diesem Abschnitt wird beschrieben, wie Sie das Arbeitsblatt für die Kundenkonfiguration dazu verwenden, die bei der Entscheidung für eine Architektur zu berücksichtigenden Dimensionierungsberechnungen und weiteren Faktoren zu vereinfachen.

Verwenden des Arbeitsblatts für die Kundenkonfiguration

Mit dem Arbeitsblatt für die Kundenkonfiguration können Sie die Kundenumgebung bewerten und die Dimensionierungsanforderungen der Umgebung berechnen.

In Tabelle 10 zeigt ein ausgefülltes Arbeitsblatt für eine Beispielkundenumgebung. Anhang A stellt ein leeres Arbeitsblatt für die Kundenkonfiguration bereit, das Sie ausdrucken und zur Lösungsdimensionierung für einen Kunden verwenden können.

Tabelle 10. Beispiel für ein Arbeitsblatt für die Kundenkonfiguration

Benutzertyp		vCPUs	Arbeitsspeicher	IOPS	Entsprechende virtuelle Referenzdesktops	Anzahl der Benutzer	Gesamtanzahl der Referenzdesktops
Benutzer mit häufiger Nutzung	Ressourcenanforderungen	2	8 GB	12	---	---	---
	Entsprechende virtuelle Referenzdesktops	2	4	2	4	200	800
Benutzer mit mittlerer Nutzung	Ressourcenanforderungen	2	4 GB	8	---	---	---
	Entsprechende virtuelle Referenzdesktops	2	2	1	2	200	400
Typische Benutzer	Ressourcenanforderungen	1	2 GB	8	---	---	---
	Entsprechende virtuelle Referenzdesktops	1	1	1	1	1200	1200
Gesamt							**2.400**

Gehen Sie beim Ausfüllen des Arbeitsblatts für die Kundenkonfiguration wie folgt vor:

1. Ermitteln Sie, für welche Benutzertypen eine Migration in die VSPEX-Anwender-Computing-Umgebung geplant ist und erfassen Sie die Menge für jeden Benutzertyp.
2. Bestimmen Sie für jeden Benutzertyp die Rechnerressourcenanforderungen hinsichtlich virtueller CPUs, Arbeitsspeicher (GB), Speicherperformance (IOPS) und Speicherkapazität.

3. Legen Sie für jeden Ressourcen- und jeden Benutzertyp die entsprechenden Anforderungen für die virtuellen Referenzdesktops fest, das heißt, die erforderliche Anzahl virtueller Referenzdesktops zur Erfüllung der angegebenen Ressourcenanforderungen.
4. Bestimmen Sie die Gesamtanzahl der Referenzdesktops, die für die Kundenumgebung aus dem Ressourcenpool benötigt werden.

Festlegen der Ressourcenanforderungen

CPU

Bei dem in Tabelle 5 auf Seite 40 dargestellten virtuellen Referenzdesktop wird davon ausgegangen, dass die meisten Desktopanwendungen für eine einzige CPU optimiert werden. Wenn für einen Benutzertyp ein Desktop mit mehreren virtuellen CPUs erforderlich ist, ändern Sie die vorgeschlagene Anzahl virtueller Desktops, um die zusätzlichen Ressourcen zu berücksichtigen. Wenn Sie beispielsweise 100 Desktops virtualisieren, aber 20 Benutzer 2 CPUs statt einer benötigen, muss Ihr Pool eine Kapazität von 120 virtuellen Desktops bereitstellen.

Arbeitsspeicher

Der Speicher spielt für die Funktion und Performance von Anwendungen eine wichtige Rolle. Deshalb sind für jede Desktopgruppe unterschiedliche Ziele hinsichtlich des verfügbaren Arbeitsspeichers erforderlich. Wenn eine Gruppe von Benutzern zusätzliche Speicherressourcen benötigt, passen Sie wie bei der CPU-Berechnung einfach die Anzahl der geplanten Desktops an, um die zusätzlichen Ressourcenanforderungen zu berücksichtigen.

Wenn Sie beispielsweise 200 Desktops virtualisieren, aber jeder Desktop 4 GB anstelle der im virtuellen Referenzdesktop bereitgestellten 2 GB Arbeitsspeicher benötigt, planen Sie für 400 virtuelle Referenzdesktops.

IOPS

Die Anforderungen an die Speicherperformance für Desktops gehören normalerweise zu den am wenigsten verstandenen Aspekten der Performance. Der virtuelle Referenzdesktop verwendet einen Workload, der von einem branchenüblichen Tool generiert wird, um eine Vielfalt von Office-Produktivitätsanwendungen auszuführen. Das sollte für die Mehrheit der virtuellen Desktopimplementierungen repräsentativ sein.

Speicherkapazität

Die Anforderungen an die Speicherkapazität für einen Desktop können je nach Typ der verwendeten Anwendungen und speziellen Kunden-Policies sehr unterschiedlich sein. Die virtuellen Desktops in dieser Lösung sind auf zusätzlichen gemeinsamen Speicher für Benutzerprofildaten und Benutzerdokumente angewiesen. Diese Anforderung ist optional und wird durch Hinzufügen von in der Lösung definierter Speicherhardware erfüllt. Sie kann auch durch vorhandene Dateifreigaben erfüllt werden.

Festlegen der entsprechenden virtuellen Referenzdesktops

Nachdem alle Ressourcen definiert wurden, bestimmen Sie mithilfe der in Tabelle 11 aufgeführten Beziehungen eine geeignete Anzahl entsprechender virtueller Referenzdesktops. Runden Sie alle Werte zur nächsthöheren Zahl auf.

Tabelle 11. Ressourcen für virtuelle Referenzdesktops

Ressource	Wert für virtuellen Referenzdesktop	Beziehung zwischen Anforderungen und entsprechenden virtuellen Referenzdesktops
CPU	1	Entsprechende virtuelle Referenzdesktops = Ressourcenanforderungen
Arbeitsspeicher	2	Entsprechende virtuelle Referenzdesktops = (Ressourcenanforderungen)/2
IOPS	10	Entsprechende virtuelle Referenzdesktops = (Ressourcenanforderungen)/10

Für den Benutzertyp mit häufiger Nutzung in Tabelle 10 auf Seite 45 sind beispielsweise zwei virtuelle CPUs, 12 IOPS und 8 GB Arbeitsspeicher für jeden Desktop erforderlich. Dies bedeutet 2 virtuelle Referenzdesktops für CPU, 4 virtuelle Referenzdesktops für Arbeitsspeicher und 2 virtuelle Referenzdesktops für IOPS.

Die Anzahl der für jeden Benutzertyp erforderlichen virtuellen Referenzdesktops entspricht dann dem für eine individuelle Ressource erforderlichen Maximum. So ist beispielsweise die Anzahl der entsprechenden virtuellen Referenzdesktops für den Benutzertyp mit häufiger Nutzung in Tabelle 10 4, da diese Zahl alle Ressourcenanforderungen an IOPS, vCPUs und Arbeitsspeicher erfüllt.

Zur Berechnung der Gesamtanzahl der Referenzdesktops für einen Benutzertyp multiplizieren Sie die Anzahl der entsprechenden virtuellen Referenzdesktops für diesen Benutzertyp mit der Anzahl der Benutzer.

Festlegen der Gesamtanzahl der virtuellen Referenzdesktops

Nachdem das Arbeitsblatt für jeden Benutzertyp, den der Kunde in die virtuelle Infrastruktur migrieren möchte, ausgefüllt ist, berechnen Sie die Gesamtanzahl der im Ressourcenpool erforderlichen virtuellen Referenzdesktops, indem Sie die Summe aller virtuellen Referenzdesktops für alle Benutzertypen berechnen. Im Beispiel in Tabelle 10 sind das insgesamt 2.400 virtuelle Desktops.

Auswählen einer Referenzarchitektur

Diese VSPEX-Referenzarchitektur für Anwender-Computing unterstützt zwei separate Skalierungspunkte mit zwei XtremIO-X-Brick-Bausteinkonfigurationen:

- Ein Starter X-Brick, der zum Hosten von virtuellen Desktops mit 1.250 vollständigen Clones oder 1.750 verknüpften Clones verwendet wurde
- Ein vollständiger X-Brick-Baustein, der zum Hosten von virtuellen Desktops mit 2.500 vollständigen Clones oder 3.500 verknüpften Clones verwendet wurde

Der Gesamtwert für virtuelle Referenzdesktops aus dem ausgefüllten Arbeitsblatt für die Kundenkonfiguration kann dafür verwendet werden zu prüfen, ob diese Referenzarchitektur den Anforderungen des Kunden entsprechen würde. Im Beispiel in Tabelle 10 auf Seite 45 benötigt der Kunde eine Kapazität von 2.400 virtuellen Desktops aus dem Pool. Daher bietet diese Referenzarchitektur ausreichend Ressourcen für die aktuellen Anforderungen und Raum für Wachstum.

Allerdings müssen eventuell andere Faktoren für die Verifizierung des ordnungsgemäßen Betriebs der Referenzarchitektur berücksichtigt werden. Beispiel:

- **Gleichzeitigkeit**

  Bei dem für die Validierung der Lösung verwendeten Workload wird davon ausgegangen, dass alle Desktopbenutzer jederzeit aktiv sind. Die Referenzarchitektur für 2.500 Desktops wurde mit 2.500 Desktops getestet, die alle parallel Workloads generieren, alle zur selben Zeit gestartet wurden und so weiter. Wenn der Kunde von 2.500 Benutzern ausgeht, von denen aber zu jedem Zeitpunkt aufgrund von Zeitzonenunterschieden oder abwechselnden Schichten nur 50 % angemeldet sind, kann die Referenzarchitektur in diesem Fall eventuell noch weitere Desktops unterstützen.

- **Höhere Desktop Workloads**

  Der Referenz-Workload wird als eine typische Last für Büromitarbeiter betrachtet. Die Benutzer einiger Kunden sind jedoch möglicherweise aktiver.

  Wenn ein Unternehmen 2.500 Benutzer hat und jeder Benutzer aufgrund der benutzerdefinierten Unternehmensanwendungen 50 IOPS (davon hauptsächlich Schreib-IOPS) anstelle der im Referenz-Workload verwendeten 10 IOPS generiert, benötigt dieser Kunde 125.000 IOPS (2.500 Benutzer x 50 IOPS pro Desktop). Diese Konfiguration wäre in diesem Fall möglicherweise nicht leistungsstark genug, da die vorgesehene I/O-Last größer als das Arraymaximum von 100.000 Schreib-IOPS ist. Das Unternehmen müsste einen zusätzlichen X-Brick-Baustein bereitstellen oder die aktuelle I/O-Last oder die Gesamtanzahl der Desktops reduzieren, um sicherzustellen, dass das Speicherarray ordnungsgemäß arbeiten kann.

Feinabstimmung der Hardwareressourcen

In den meisten Fällen wird mit dem Arbeitsblatt für die Kundenkonfiguration eine Referenzarchitektur vorgeschlagen, die für die Anforderungen des Kunden ausreicht. In einigen Fällen kann es jedoch sinnvoll sein, wenn Sie die für das System verfügbaren Hardwareressourcen weiter anpassen. Eine vollständige Beschreibung der Systemarchitektur würde über den Rahmen dieses Dokuments hinausgehen, aber in den folgenden Kapiteln erfahren Sie, wie Sie an diesem Punkt zusätzliche Anpassungen der Lösung vornehmen können.

Speicherressourcen

Diese Lösung besteht aus zwei separaten XtremIO-X-Brick-Bausteinkonfigurationen, einem Starter-X-Brick-Baustein, um entweder virtuelle Desktops mit bis zu 1.250 vollständigen Clones oder 1.750 verknüpften Clones zu unterstützen, und einem X-Brick-Baustein, um entweder virtuelle Desktops mit bis zu 2.500 vollständigen Clones oder 3.500 verknüpften Clones zu unterstützen.

XtremIO-X-Brick-Bausteine sind für den Support einer höheren Anzahl von Desktops (mit vollständigen und mit verknüpften Clones) validiert und die Zahlen der VSPEX-Validierungen gelten nur für die hier vorgestellte Lösung.

Das XtremIO-Array erfordert kein Tuning und die Anzahl der verfügbaren SSDs im Array ist festgelegt. Überprüfen Sie anhand des VSPEX-Dimensionierungstools oder des Arbeitsblatts für die Kundenkonfiguration, ob das EMC XtremIO-Array die erforderlichen Kapazitäts- und Performancelevel liefern kann.

Serverressourcen

Im Hinblick auf die Serverressourcen in der Lösung können die Hardwareressourcen effektiver angepasst werden. Bestimmen Sie dazu zunächst die gesamten Ressourcenanforderungen für die Serverkomponenten, wie in Tabelle 12 gezeigt. Notieren Sie die Summe der Spalten **Total CPU Resources** und **Total memory Resources** im Arbeitsblatt.

Tabelle 12. Gesamtanzahl der Serverressourcenkomponenten

Anwendertypen		vCPUs	Arbeitsspeicher (GB)	Anzahl der Benutzer	Gesamt-CPU-Ressourcen	Gesamtspeicherressourcen
Benutzer mit häufiger Nutzung	Ressourcenanforderungen	2	8	200	400	1.600
Benutzer mit mittlerer Nutzung	Ressourcenanforderungen	2	4	200	400	800
Typische Benutzer	Ressourcenanforderungen	1	2	1200	1200	2.400
Gesamt					**2.000**	**4.800**

Für das Beispiel in Tabelle 12 sind 2.000 virtuelle CPUs und 4.800 GB Arbeitsspeicher erforderlich. Die Referenzarchitektur rechnet mit 5 Desktops pro physischen Prozessorkern und keinem übermäßigen Provisioning von Speicher, wodurch sich daraus in diesem Fall 500 physische Prozessorkerne und 4.800 GB Speicher ergeben. Diese Werte können dazu verwendet werden, die insgesamt erforderlichen Serverressourcen genauer zu ermitteln.

Hinweis: Berücksichtigen Sie bei der Anpassung der Hardware für den Ressourcenpool auch die Anforderungen an die hohe Verfügbarkeit.

Übersicht

EMC betrachtet die in der Lösung angegebenen Anforderungen als die Mindestressourcen, die für die Verarbeitung der Workloads basierend auf der angegebenen Definition eines virtuellen Referenzdesktops erforderlich sind. In einer Kundenimplementierung ändert sich die Systemlast im Laufe der Zeit abhängig davon, wie Benutzer mit dem System interagieren. Wenn die virtuellen Desktops des Kunden erheblich von der Referenzdefinition abweichen und in einer Ressourcengruppe nicht homogen sind, müssen Sie dem System möglicherweise mehr dieser Ressource hinzufügen.

Kapitel 5 Überlegungen und Best Practices für das Lösungsdesign

In diesem Kapitel werden die folgenden Themen behandelt:

Übersicht 52

Überlegungen zum Serverdesign 52

Überlegungen zum Netzwerkdesign 59

Überlegungen zum Speicherdesign 64

Hohe Verfügbarkeit und Failover 66

Profil der Validierungstests 69

Virenschutz- und Anti-Malware-Plattformprofil 70

VMware vRealize Operations Manager für Horizon View – Plattformprofil 70

VSPEX-Lösung für VMware Workspace 71

Übersicht

Dieses Kapitel beschreibt Best Practices und Überlegungen für das Design der VSPEX-Lösung für Anwender-Computing. Weitere Informationen zu Best Practices für die Bereitstellung verschiedener Komponenten der Lösung finden Sie in der anbieterspezifischen Dokumentation.

Überlegungen zum Serverdesign

EMC entwirft VSPEX-Lösungen, die auf die Ausführung auf vielen verschiedenen Serverplattformen ausgelegt sind. VSPEX definiert die mindestens erforderlichen CPU- und Arbeitsspeicherressourcen, jedoch nicht einen bestimmten Servertyp oder eine bestimmte Konfiguration. Der Kunde kann jede Serverplattform und -konfiguration verwenden, die die Mindestanforderungen erfüllt oder übertrifft.

In Abbildung 8 sehen Sie beispielsweise, wie ein Kunde dieselben Serveranforderungen entweder mithilfe von White-Box-Servern oder High-End-Servern implementieren kann. Beide Implementierungen erreichen die erforderliche Anzahl an Prozessorkernen und die benötigte RAM-Menge, aber die Anzahl und der Typ der Server unterscheiden sich.

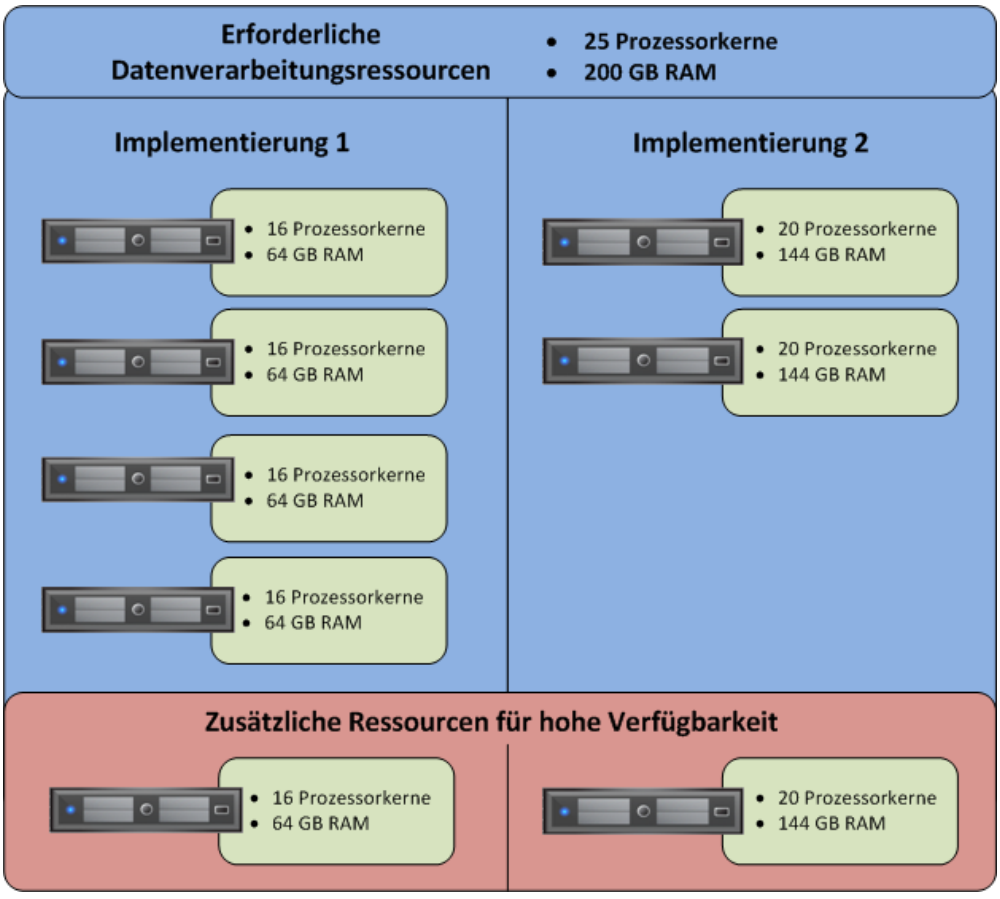


Abbildung 8. Flexibilität der Rechnerebene

Die Wahl einer Serverplattform hängt nicht nur von den technischen Anforderungen der Umgebung ab, sondern auch von der Unterstützbarkeit der Plattform, vorhandenen Beziehungen zum Serveranbieter, erweiterten Performance- und Managementfunktionen sowie weiteren Faktoren. Beispiel:

- Aus Virtualisierungssicht können Funktionen wie Arbeitsspeichererweiterung (Ballooning) und die transparente gemeinsame Nutzung von Arbeitsspeicherseiten den gesamten Speicherbedarf reduzieren, wenn der Workload eines Systems bekannt ist.
- Wenn der Pool der virtuellen Maschinen keine hohe Spitzenauslastung oder gleichzeitige Nutzung aufweist, können Sie die Anzahl der virtuellen CPUs reduzieren. Andererseits müssen die vCPUs und der Arbeitsspeicher möglicherweise aufgestockt werden, wenn die bereitgestellten Anwendungen viel Rechenleistung erfordern.

Die Serverinfrastruktur muss folgende Mindestanforderungen erfüllen:

- Ausreichend CPU-Kerne und Arbeitsspeicher zum Support der erforderlichen Anzahl und Art von virtuellen Maschinen
- Ausreichend Netzwerkverbindungen, um redundante Konnektivität der Systemswitche zu ermöglichen
- Ausreichend überschüssige Kapazität, damit die Umgebung einen Serverausfall und ein Failover überstehen kann

Best Practices für Server

Für diese Lösung empfiehlt EMC die Berücksichtigung folgender Best Practices für die Serverebene:

- **Verwendung identischer Servereinheiten**

  Verwenden Sie identische oder zumindest kompatible Server, damit ähnliche Hardwarekonfigurationen genutzt werden. Bei VSPEX werden Technologien für hohe Verfügbarkeit auf Hypervisor-Ebene implementiert, die ähnliche Instruktionssätze auf der zugrunde liegenden physischen Hardware erfordern können. Durch die Implementierung von VSPEX auf identischen Servereinheiten können Kompatibilitätsprobleme in diesem Bereich auf ein Minimum begrenzt werden.

- **Verwendung aktueller Prozessortechnologien**

  Verwenden Sie für neue Bereitstellungen aktuelle Versionen gängiger Prozessortechnologien. Dabei wird davon ausgegangen, dass deren Performance ebenso gut oder besser ist als die für die Validierung der Lösung verwendeten Systeme.

- **Implementierung von hoher Verfügbarkeit zum Abfangen von Ausfällen eines einzelnen Servers**

  Implementieren Sie die verfügbaren Funktionen für hohe Verfügbarkeit in der Virtualisierungsebene und achten Sie darauf, dass die Rechnerebene genügend Ressourcen hat, um den Ausfall von einem Server aufzufangen. Damit können Sie zudem Upgrades mit minimaler Ausfallzeit implementieren. Hohe Verfügbarkeit und Failover enthält weitere Details.

  Hinweis: Wenn Sie hohe Verfügbarkeit auf der Hypervisor-Ebene implementieren, hängt die Größe der größten virtuellen Maschine, die Sie erstellen können, vom kleinsten physischen Server in der Umgebung ab.

- **Monitoring der Ressourcenauslastung und Anpassung nach Bedarf**

  Beispielsweise wird bei dem virtuellen Referenzdesktop und den erforderlichen Hardwareressourcen in dieser Lösung davon ausgegangen, dass nicht mehr als fünf virtuelle CPUs für jeden physischen Prozessorkern vorhanden sind (Verhältnis von 5:1). In den meisten Fällen bietet dies ausreichend Ressourcen für die gehosteten virtuellen Desktops, aber das Verhältnis ist möglicherweise nicht für alle Anwendungsbeispiele angemessen. EMC empfiehlt, die CPU-Auslastung auf der Hypervisor-Ebene zu überwachen, um bestimmen zu können, ob weitere Ressourcen erforderlich sind, und diese dann nach Bedarf hinzuzufügen.

Validierte Serverhardware

In Tabelle 13 zeigt die in dieser Lösung validierte Serverhardware und die Konfigurationen.

Tabelle 13. Serverhardware

Server für virtuelle Desktops	Konfiguration
CPU	• 1 vCPU pro Desktop (5 Desktops pro Kern) • 250 Kerne für alle Server bei 1.250 virtuellen Desktops • 350 Kerne für alle Server bei 1.750 virtuellen Desktops • 500 Kerne für alle Server bei 2.500 virtuellen Desktops • 700 Kerne für alle Server bei 3.500 virtuellen Desktops
Arbeitsspeicher	• 2 GB RAM pro virtuelle Maschine • 2,5 TB RAM für alle Server bei 1.250 virtuellen Desktops • 3,5 TB RAM für alle Server bei 1.750 virtuellen Desktops • 5 TB RAM für alle Server bei 2.500 virtuellen Desktops • 7 TB RAM für alle Server bei 3.500 virtuellen Desktops • 2 GB RAM Reservierung pro vSphere-Host
Netzwerk	• Drei 10-GbE-NICs pro Blade-Gehäuse oder sechs 1-GbE-NICs pro eigenständigen Server

Hinweise:

- Das 5:1-Verhältnis zwischen virtuellen CPUs und physischen Kernen gilt für den in diesem Designleitfaden definierten Referenz-Workload. Bei der Bereitstellung von VMware vShield Endpoint oder Avamar fügen Sie CPUs und RAM nach Bedarf für CPU- und RAM-intensive Komponenten hinzu. Informationen zu den Ressourcenanforderungen für vShield Endpoint und Avamar finden Sie in der entsprechenden Produktdokumentation.

- Zusätzlich zu den Servern, die Sie bereitstellen, um die Mindestanforderungen in Tabelle 13 zu erfüllen, müssen Sie der Infrastruktur einen zusätzlichen Server hinzufügen, um Support für VMware vSphere HA zu bieten.

vSphere-Speichervirtualisierung

vSphere verfügt über eine Reihe von erweiterten Funktionen, mit denen die Performance und die allgemeine Ressourcenauslastung optimiert werden können. In diesem Abschnitt werden die wichtigsten Funktionen für das Speichermanagement und Überlegungen zu deren Verwendung in Ihrer VSPEX-Lösung beschrieben.

Abbildung 9 zeigt, wie ein einzelner Hypervisor Speicher von einem Ressourcenpool belegt. vSphere-Speichermanagementfunktionen wie Überbelegung von Speicher, transparente gemeinsame Nutzung von Arbeitsspeicherseiten und Arbeitsspeicherzunahme können die Gesamtspeicherbelegung verringern und die Konsolidierungsraten im Hypervisor erhöhen.

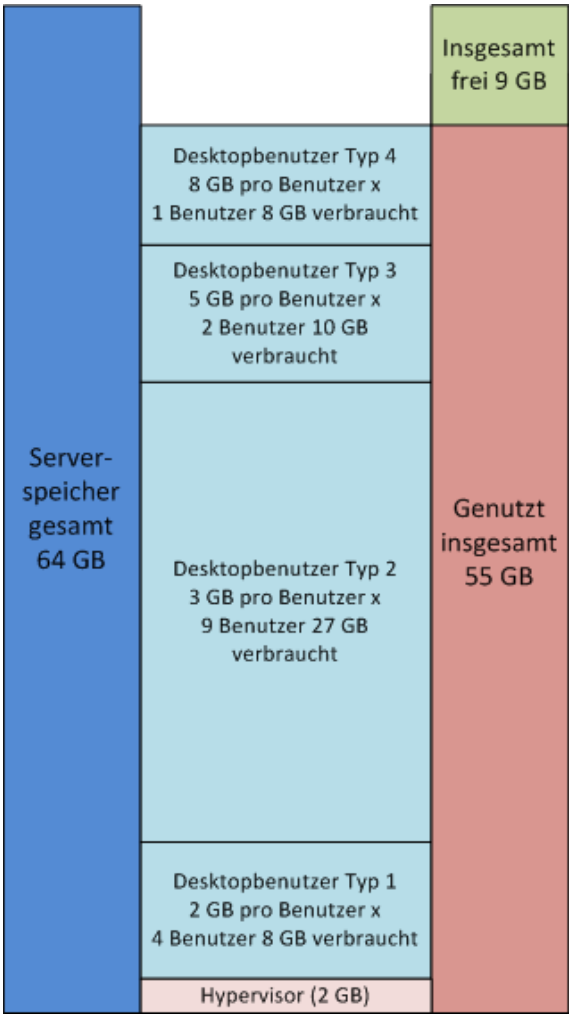

Insgesamt frei 9 GB
Desktopbenutzer Typ 4
8 GB pro Benutzer x
1 Benutzer 8 GB verbraucht
Desktopbenutzer Typ 3
5 GB pro Benutzer x
2 Benutzer 10 GB verbraucht
Server-speicher gesamt 64 GB
Desktopbenutzer Typ 2
3 GB pro Benutzer x
9 Benutzer 27 GB verbraucht
Genutzt insgesamt 55 GB
Desktopbenutzer Typ 1
2 GB pro Benutzer x
4 Benutzer 8 GB verbraucht
Hypervisor (2 GB)

Abbildung 9. Speicherbelegung durch Hypervisor

Der vSphere-Hypervisor kann mithilfe von Verfahren zur Arbeitsspeichervirtualisierung physische Hostressourcen wie Arbeitsspeicher abstrahieren, um Ressourcen auf mehreren virtuellen Maschinen zu isolieren, ohne diese völlig zu erschöpfen. Wenn fortschrittliche Prozessoren (z. B. Intel-Prozessoren mit EPT-Support) bereitgestellt werden, erfolgt diese Speicherabstrahierung in der CPU. Andernfalls findet dies mittels Shadow Page Tables im Hypervisor statt.

vSphere bietet die folgenden Techniken für das Arbeitsspeichermanagement:

- **Überbelegung von Speicher**

  Zu einer Überbelegung von Speicher kommt es, wenn den virtuellen Maschinen mehr Speicher zugeteilt wird, als physisch auf einem VMware vSphere-Host vorhanden ist. Mithilfe von fortschrittlichen Methoden wie Arbeitsspeichererweiterung (Ballooning) und der transparenten gemeinsamen Nutzung von Arbeitsspeicherseiten kann vSphere eine Überbelegung von Speicher ausgleichen, ohne dass es zu einer Performanceverschlechterung kommt. Wenn jedoch mehr Arbeitsspeicher verwendet wird, als auf dem Server vorhanden ist, lagert vSphere möglicherweise Teile des Arbeitsspeichers einer virtuellen Maschine aus.

- **Non-Uniform Memory Access (NUMA)**

  vSphere verwendet einen NUMA-Lastenausgleich, um einer virtuellen Maschine einen Stamm-Node zuzuweisen. Der Speicherzugriff ist lokal und ermöglicht so eine optimale Performance, da der Speicher der virtuellen Maschine vom Stammknoten aus zugewiesen wird. Auch Anwendungen, die NUMA nicht direkt unterstützen, profitieren von dieser Funktion.

- **Transparente gemeinsame Nutzung von Arbeitsspeicherseiten**

  Virtuelle Maschinen, auf denen ähnliche Betriebssysteme und Anwendungen ausgeführt werden, verfügen normalerweise über ähnlichen Speicherinhalt. Bei der gemeinsamen Nutzung von Arbeitsspeicherseiten kann sich der Hypervisor redundante Kopien zurückholen und dem Host für die erneute Nutzung freigeben.

- **Arbeitsspeicherkomprimierung**

  Durch die Arbeitsspeicherkomprimierung speichert vSphere Seiten, die andernfalls auf das Laufwerk durch Host-Swapping ausgelagert würden, in einem Komprimierungscache im Hauptarbeitsspeicher.

- **Arbeitsspeichererweiterung (Ballooning)**

  Dies beugt der Erschöpfung der Hostressourcen vor, indem freie Seiten von der virtuellen Maschine dem Host zur Wiederverwendung ohne bzw. mit geringen Auswirkungen auf die Performance der Anwendung zugewiesen werden.

- **Hypervisor-Swapping**

  Dadurch kann der Host dazu veranlasst werden, willkürliche Seiten von virtuellen Maschinen auf Festplatten auszulagern.

Weitere Informationen finden Sie im VMware White Paper *Management von Arbeitsspeicherressourcen in VMware vSphere 5.0*.

Richtlinien für die Arbeitsspeicherkonfiguration

Die korrekte Dimensionierung und Konfiguration der Lösung setzt eine entsprechende Sorgfalt bei der Konfiguration des Serverspeichers voraus. In diesem Abschnitt finden Sie Richtlinien für die Arbeitsspeicherzuweisung zu virtuellen Maschinen. Dabei werden der vSphere-Arbeitsspeicher-Overhead und die Arbeitsspeichereinstellungen der virtuellen Maschine berücksichtigt.

vSphere-Arbeitsspeicher-Overhead

Ein gewisser Anteil an Arbeitsspeicher-Overhead ist der Virtualisierung von Arbeitsspeicherressourcen zugeordnet. Dieser Overhead umfasst zwei Komponenten:

- System-Overhead für den VMkernel
- Zusätzlicher Overhead für jede einzelne virtuelle Maschine

Der Overhead für den VMkernel ist konstant, für die einzelnen virtuellen Maschinen hängt er dagegen von der Anzahl der virtuellen CPUs und dem konfigurierten Arbeitsspeicher für das Gastbetriebssystem ab.

Arbeitsspeichereinstellungen für virtuelle Maschinen

Abbildung 10 zeigt die Parameter der Arbeitsspeichereinstellungen für die virtuelle Maschine, z. B.:

- **Configured Memory (Konfigurierter Speicher):** Physischer Speicher, der der virtuellen Maschine bei der Erstellung zugeteilt wird.
- **Reserved memory (reservierter Arbeitsspeicher):** der virtuellen Maschine garantierter Arbeitsspeicher
- **Touched Memory (belegter Speicher):** Speicher, der aktiv ist oder von der virtuellen Maschine verwendet wird.
- **Swappable (Auslagerbar):** Arbeitsspeicher, der der virtuellen Maschine entzogen werden kann, wenn der Host aufgrund von Arbeitsspeichererweiterungen, Komprimierung oder Auslagerung bei anderen virtuellen Maschinen weiteren Arbeitsspeicher benötigt.

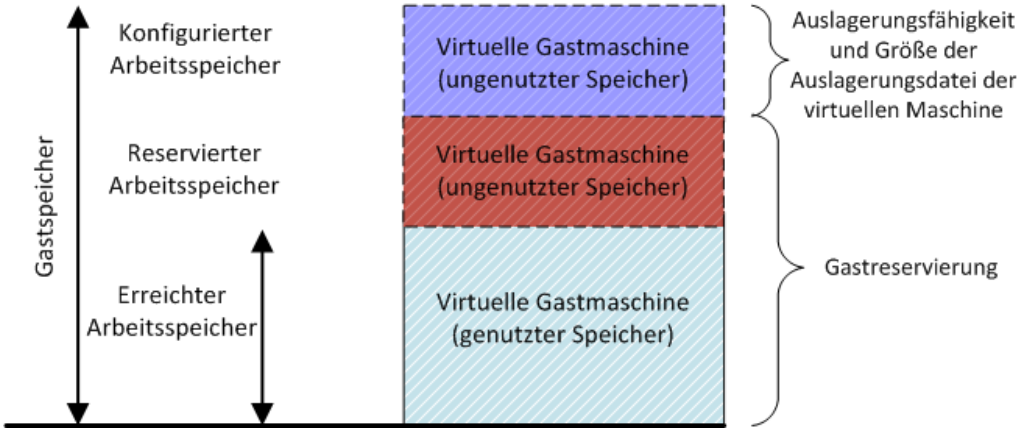


Abbildung 10. Arbeitsspeichereinstellungen für virtuelle Maschinen

EMC empfiehlt, die folgenden Best Practices für die Speichereinstellungen der virtuellen Maschine zu befolgen:

- Deaktivieren Sie die Standardmethoden zum Freisetzen von Speicher nicht. Diese einfachen Prozesse haben eine minimale Auswirkung auf Workloads.

- Teilen Sie Arbeitsspeicher für virtuelle Maschinen durchdacht zu.

  Bei einer zu großzügigen Zuteilung werden Ressourcen nicht optimal genutzt, während eine zu knappe Zuteilung zu Performanceeinbußen führt, die sich auf andere virtuelle Maschinen mit gemeinsam genutzten Ressourcen auswirken können. Eine Überbelegung kann eine Ressourcenerschöpfung nach sich ziehen, wenn der Hypervisor nicht mehr Arbeitsspeicherressourcen bereitstellen kann. In extremen Fällen kann es bei Hypervisor-Swapping zu Performanceeinbußen bei den virtuellen Maschinen kommen.

  Hier sind Performance-Baselines für die Workloads von virtuellen Maschinen hilfreich.

Zuteilen von Arbeitsspeicher für virtuelle Maschinen

Die Serverkapazität ist in der Lösung für zwei Zwecke erforderlich:

- Zum Support der erforderlichen Infrastrukturservices wie Authentifizierung/Autorisierung, DNS und Datenbank

  Weitere Informationen zu den Hosting-Anforderungen für diese Infrastrukturservices finden Sie im VSPEX Proven Infrastructure-Leitfaden zur Private Cloud, der unter Grundlegende Dokumente aufgeführt ist.

- So unterstützen Sie die virtualisierte Desktopinfrastruktur:

  In dieser Lösung hat jeder virtuelle Desktop 2 GB Arbeitsspeicher, wie in Tabelle 5 auf Seite 40 definiert. Diese Lösung wurde mit statisch zugewiesenem Arbeitsspeicher und ohne Überbelegung von Arbeitsspeicherressourcen validiert. Wenn eine Speicherüberschreitung in einer realen Umgebung verwendet wird, überwachen Sie die Systemspeicherauslastung und die damit verbundene Auslagerungsdatei-I/O-Aktivität regelmäßig, damit es nicht zu einer Speicherlücke kommt, die unerwartete Ergebnisse nach sich ziehen kann.

Überlegungen zum Netzwerkdesign

VSPEX-Lösungen definieren die Mindestanforderungen für das Netzwerk und bieten allgemeine Anweisungen zur Netzwerkarchitektur, ermöglichen es Kunden jedoch, beliebige Netzwerkhardware auszuwählen, die diese Anforderungen erfüllt. Wenn zusätzliche Bandbreite benötigt wird, müssen Ressourcen sowohl für das Speicherarray als auch für den Hypervisor-Host hinzugefügt werden, um die Anforderungen zu erfüllen. Die Optionen für die Netzwerkverbindung mit dem Server hängen vom Servertyp ab.

Für Referenzzwecke in der validierten Umgebung geht EMC davon aus, dass jeder virtuelle Desktop 10 IOPS mit einer durchschnittlichen Größe von 4 KB erzeugt. Das bedeutet, dass jeder virtuelle Desktop mindestens 40 KB/s Datenverkehr im Speichernetzwerk generiert. Bei einer für 1.250 virtuelle Desktops bewerteten Umgebung bedeutet dies ein Minimum von etwa 50 MB/s, was für moderne Netzwerke kein Problem ist, hierbei werden jedoch keine anderen Vorgänge berücksichtigt. Zusätzliche Bandbreite ist für Folgendes erforderlich:

- Benutzernetzwerkverkehr
- Virtuelle Desktopmigration
- Administrative und Managementvorgänge

Die jeweiligen Anforderungen sind je nach Umgebung unterschiedlich. Es empfiehlt sich deshalb nicht, in diesem Zusammenhang konkrete Zahlen anzugeben. Die in den Referenzarchitekturen für jede Lösung beschriebenen Netzwerke sollten jedoch ausreichend sein, um durchschnittliche Workloads in diesen Vorgängen zu verarbeiten.

Unabhängig von den Anforderungen an den Netzwerkdatenverkehr sollten immer mindestens zwei physische Netzwerkverbindungen gemeinsam in einem logischen Netzwerk aufrechterhalten werden, damit der Ausfall einer Verbindung sich nicht auf die Verfügbarkeit des Systems auswirkt. Das Netzwerk muss so ausgelegt sein, dass die verfügbare gesamte Bandbreite ausreicht, um bei einem Ausfall die gesamte Workload zu unterstützen.

Die Netzwerkinfrastruktur muss folgende Anforderungen erfüllen:

- Redundante Netzwerkverbindungen für Hosts, Switche und Speicher
- Support für Linkzusammenfassung
- Datenverkehrsisolierung anhand von Branchen-Best-Practices

Validierte Netzwerkhardware

In Tabelle 14 zeigt die Hardwareressourcen für die in dieser Lösung validierte Netzwerkinfrastruktur.

Tabelle 14. Switching-Kapazität (Minimum)

Speichertyp	Konfiguration
XtremIO für virtuellen Desktopspeicher	• 2 physische Switche • 2 FC/FCoE/10GbE-Ports pro VMware vSphere-Server für das Speichernetzwerk • 2 FC/10-GbE-Ports pro SC für Desktopdaten
VNX für optionalen Benutzerdatenspeicher	• 2 physische Switche • 2 10-GbE-Ports pro vSphere-Server • 1 1-GbE-Port pro Control Station für Management • 2 10-GbE-Ports pro Data Mover für Daten
Isilon für optionalen Benutzerdatenspeicher	• 2 physische Switche • 2 10-GbE-Ports pro vSphere-Server • 1 1-GbE-Port pro Node für Management • 2 10-GbE-Ports pro Data Mover für Daten

Hinweise:

- Für die Lösung kann eine 1-GbE-Netzwerkinfrastruktur verwendet werden, sofern die zugrunde liegenden Anforderungen an Bandbreite und Redundanz erfüllt sind.
- Für diese Konfiguration wird davon ausgegangen, dass die VSPEX-Implementierung Rack-montierte Server verwendet. Vergewissern Sie sich für auf Blade-Servern basierende Implementierungen, dass ähnliche Möglichkeiten für Bandbreite und hohe Verfügbarkeit zur Verfügung stehen.

Richtlinien für die Netzwerkkonfiguration

Dieser Abschnitt enthält Richtlinien für das Konfigurieren eines redundanten Netzwerks mit hoher Verfügbarkeit. Für die Richtlinien werden Netzwerkredundanz, Linkzusammenfassung, Datenverkehrsisolierung und Jumbo Frames berücksichtigt.

Die Konfigurationsbeispiele gelten für IP-basierte Netzwerke, aber für FC-Speichernetzwerke werden ähnliche Best Practices und Designrichtlinien angewendet.

Netzwerkredundanz

Das Infrastrukturnetzwerk erfordert redundante Netzwerkverbindungen für jeden vSphere-Host, das Speicherarray, die Switchverbindungsports und die Switch-Uplink-Ports. Diese Konfiguration stellt sowohl Redundanz als auch zusätzliche Netzwerkbandbreite bereit. Diese Konfiguration ist erforderlich, unabhängig davon, ob die Netzwerkinfrastruktur für die Lösung bereits vorhanden ist oder zusammen mit anderen Komponenten der Lösung bereitgestellt wird.

In Abbildung 11 werden Beispiele für hoch verfügbare Speichernetzwerktopologien dargestellt.

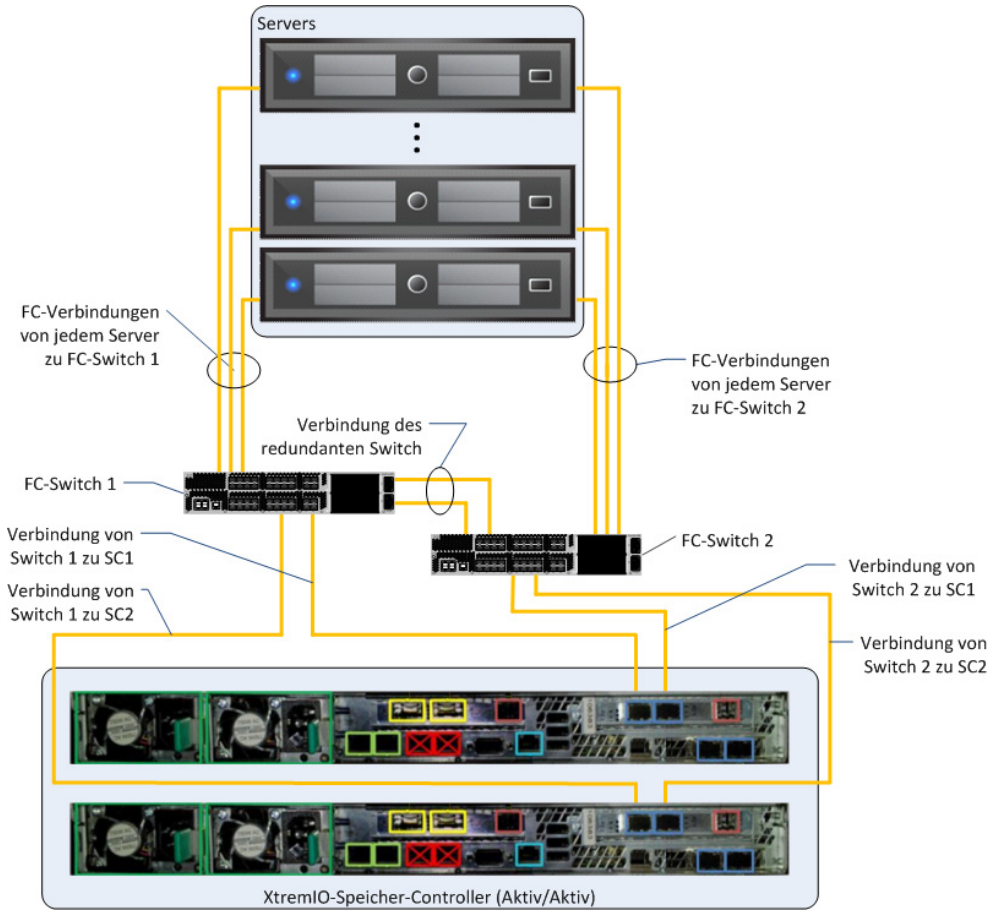

Servers
FC-Verbindungen von jedem Server zu FC-Switch 1
FC-Verbindungen von jedem Server zu FC-Switch 2
Verbindung des redundanten Switch
FC-Switch 1
FC-Switch 2
Verbindung von Switch 1 zu SC1
Verbindung von Switch 1 zu SC2
Verbindung von Switch 2 zu SC1
Verbindung von Switch 2 zu SC2
XtremIO-Speicher-Controller (Aktiv/Aktiv)

Abbildung 11. Beispiel eines XtremIO FC-Netzwerkdesigns mit hoher Verfügbarkeit

In Abbildung 12 wird ein Beispiel für eine Netzwerkeinrichtung mit hoher Verfügbarkeit für Benutzerdaten mit einem Speicherarray der VNX-Produktreihe dargestellt. Dieselben Prinzipien für hohe Verfügbarkeit gelten auch für eine Isilon-Konfiguration. In beiden Fällen hat jeder Node zwei Links zu den Switchen.

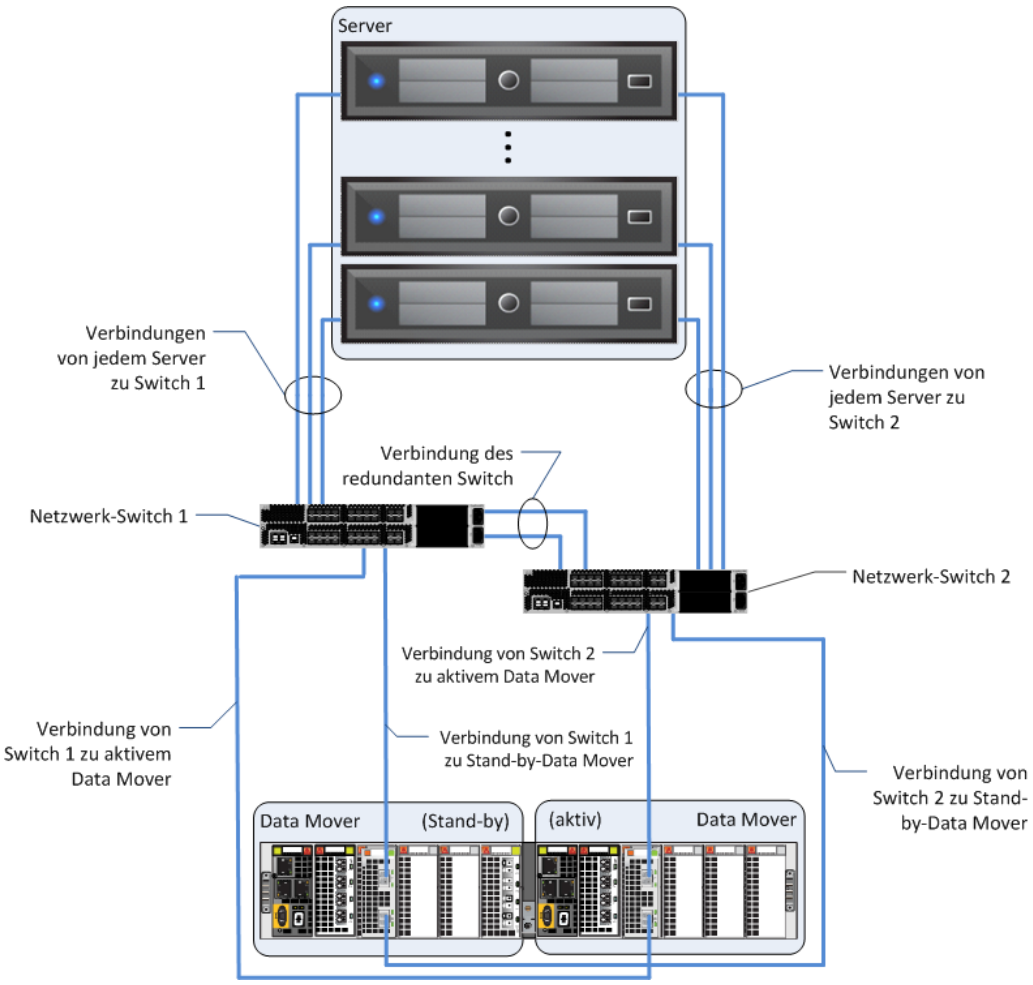

Server
Verbindungen von jedem Server zu Switch 1
Verbindungen von jedem Server zu Switch 2
Verbindung des redundanten Switch
Netzwerk-Switch 1
Netzwerk-Switch 2
Verbindung von Switch 2 zu aktivem Data Mover
Verbindung von Switch 1 zu aktivem Data Mover
Verbindung von Switch 1 zu Stand-by-Data Mover
Verbindung von Switch 2 zu Stand-by-Data Mover
Data Mover
(Stand-by)
(aktiv)
Data Mover

Abbildung 12. Beispiel eines VNX Ethernet-Netzwerkdesigns mit hoher Verfügbarkeit

Verbindungsbündelung

VNX und Isilon bieten hohe Netzwerkverfügbarkeit oder Redundanz durch Linkzusammenfassung. Bei der Linkzusammenfassung können mehrere aktive Ethernetverbindungen als ein Link mit einer einzigen MAC-Adresse und potenziell mehreren IP-Adressen angezeigt werden[3].

In dieser Lösung wird das LACP (Link Aggregation Control Protocol) auf dem VNX- oder Isilon-Array so konfiguriert, dass mehrere Ethernetports in einem einzigen virtuellen Gerät zusammengefasst werden. Wenn eine Verbindung in diesem Ethernetport unterbrochen wird, erfolgt ein Failover auf einen anderen Port. Wir haben den gesamten Netzwerkdatenverkehr über die aktiven Verbindungen verteilt.

Datenverkehrsisolierung

In dieser Lösung wird der unterschiedliche Netzwerkdatenverkehr durch virtuelle LANs (VLANs) getrennt, um Durchsatz, Management, Anwendungstrennung, hohe Verfügbarkeit und Sicherheit zu verbessern.

[3] Eine Linkzusammenfassung funktioniert ähnlich wie ein Ethernetkanal, es wird jedoch der LACP-Standard IEEE 802.3ad verwendet. Dieser Standard unterstützt Linkzusammenfassungen mit zwei oder mehr Ports. Alle Ports in der Aggregation müssen über dieselbe Geschwindigkeit verfügen und Vollduplexports sein.

Virtuelle LANs teilen den Netzwerkdatenverkehr auf, damit unterschiedliche Datenverkehrstypen über isolierte Netzwerke übertragen werden können. In einigen Fällen ist aufgrund gesetzlicher Bestimmungen oder aus Gründen der Policy-Compliance eine physische Isolierung erforderlich. Oft ist die logische Isolierung mittels VLANs jedoch ausreichend.

Für diese Lösung sind mindestens zwei VLANs für Clientzugriff und -management erforderlich.

In Abbildung 13 wird das Design dieser VLANs mit VNX dargestellt. Für eine Isilon-Konfiguration gelten dieselben Designprinzipien.

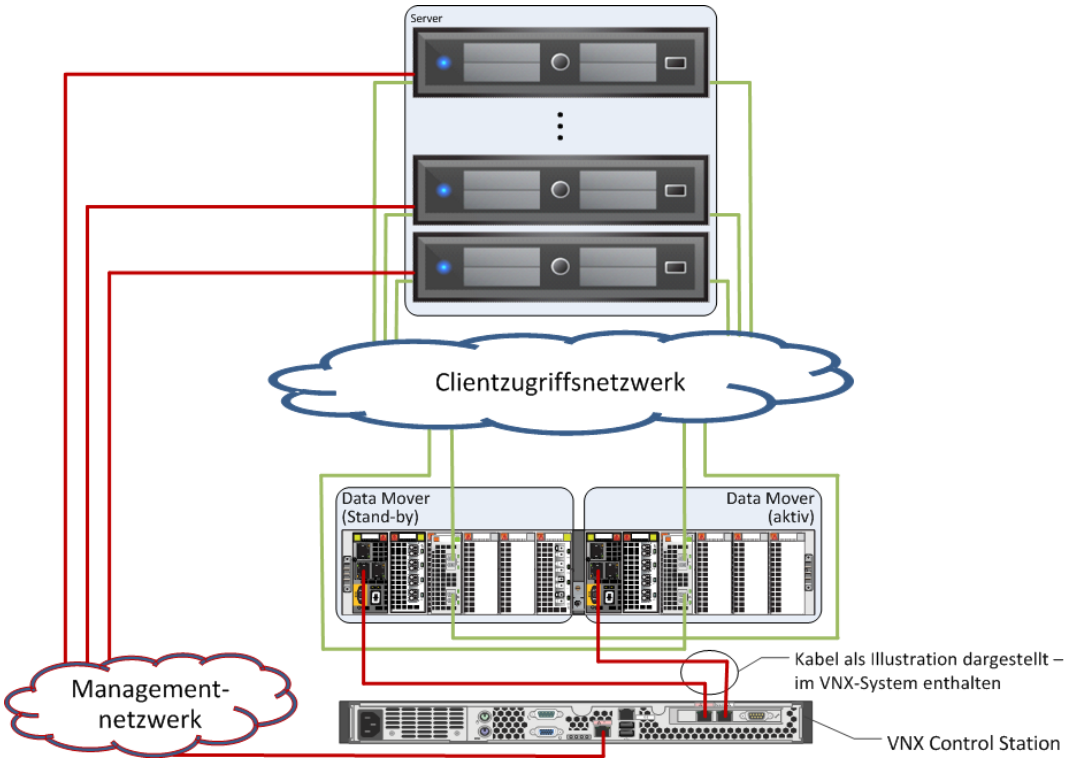


Abbildung 13. Erforderliche Netzwerke

Das Clientzugriffsnetzwerk ermöglicht es Benutzern des Systems oder Clients, mit der Infrastruktur, einschließlich der virtuellen Maschinen und den CIFS-Shares, die vom VNX- oder Isilon-Array gehostet werden, zu kommunizieren. Das Managementnetzwerk stellt für Administratoren einen dedizierten Zugriff auf die Managementverbindungen auf dem Speicherarray, den Netzwerkswitchen und den Hosts bereit.

Einige Best Practices erfordern eine zusätzliche Netzwerkisolierung für Clusterdatenverkehr, die Kommunikation auf der Virtualisierungsebene und andere Funktionen. Sie können zusätzliche Netzwerke implementieren, die jedoch nicht erforderlich sind.

Hinweis: In dieser Abbildung werden die Anforderungen an die Netzwerkverbindung für ein VNX-Array mit 10-GbE-Netzwerkverbindungen dargestellt. Erstellen Sie eine ähnliche Topologie, wenn Sie 1-GbE-Netzwerkverbindungen verwenden.

Überlegungen zum Speicherdesign

Überblick

XtremIO bietet Funktionen wie Inline-Deduplizierung, Inline-Komprimierung, Inline-Security-at-Rest und natives Thin Provisioning. Aufgrund der Speicherplanung müssen Sie Folgendes festlegen:

- Größe des Volumes
- Anzahl Volumes
- Performanceanforderungen

Jedes Volume muss größer sein als der vom Server erforderliche logische Speicherplatz. Ein XtremIO-Cluster kann die Performanceanforderungen der Lösung erfüllen.

Validierte Speicherhardware und -konfiguration

Es gibt mehrere Möglichkeiten, wie bei vSphere Speicher verwendet werden kann, wenn virtuelle Maschinen gehostet werden. Wir haben die in Abbildung 3 beschriebenen Konfigurationen mit FC getestet und die beschriebenen Speicherlayouts entsprechen allen aktuellen Best Practices. Kunden oder Architekten mit entsprechendem Hintergrundwissen und entsprechender Schulung können auf Grundlage ihrer Kenntnisse der Systemverwendung und -last ggf. Änderungen vornehmen.

Tabelle 15. Speicherhardware

Zweck	Konfiguration
Gemeinsamer XtremIO-Speicher	Gemeinsamkeiten: • 2 FC- und 2 10-GbE-Schnittstellen pro Speicher-Controller • 1 1-GbE-Schnittstelle pro Speicher-Controller für Management Für virtuelle Desktops mit 1.250 vollständigen Clones oder 1.750 verknüpften Clones: • Starter-X-Brick-Konfiguration mit 13 400-GB-Flashlaufwerken Für virtuelle Desktops mit 2.500 vollständigen Clones oder 3.500 verknüpften Clones: • X-Brick-Konfiguration mit 25 400-GB-Flashlaufwerken
Optional; gemeinsame Isilon-Speicherlaufwerkskapazität	Nur erforderlich, wenn ein Isilon-Cluster bereitgestellt wird, um Benutzerdaten zu hosten. • 3 X410-Nodes • 2 EFD-Laufwerke mit 800 GB • 34 SATA-Laufwerke mit 1 TB

Zweck	Konfiguration
Optional; gemeinsame VNX-Speicher-Laufwerkskapazität	Für virtuelle Desktops mit 1.250 vollständigen Clones: • 2 EFD-Laufwerke mit 200 GB • 16 x 2 TB NL SAS Für virtuelle Desktops mit 1.750 verknüpften Clones: • 2 EFD-Laufwerke mit 200 GB • 32 NL-SAS-Laufwerke mit 2 TB Virtuelle Desktops mit 2.500 vollständigen Clones • 4 EFD-Laufwerke mit 200 GB • 40 x 2 TB NL SAS 2.500 virtuelle persistente verknüpfte Clone-Desktops • 4 EFD-Laufwerke mit 200 GB • 48 x 2 TB NL SAS

vSphere-Speichervirtua-lisierung

Dieser Abschnitt enthält Richtlinien für das Einrichten der Speicherebene der Lösung, um hohe Verfügbarkeit bereitzustellen und das erwartete Performancelevel zu ermöglichen.

VMware vSphere ermöglicht Speichervirtualisierung auf Hostebene. Physische Speichermedien werden virtualisiert und für virtuelle Maschinen bereitgestellt.

Die virtuelle Maschine speichert ihr Betriebssystem und alle anderen mit den Aktivitäten der virtuellen Maschine in Zusammenhang stehenden Aktivitäten auf einem virtuellen Laufwerk. Das virtuelle Laufwerk kann aus einer oder mehreren Dateien bestehen. VMware greift auf den virtuellen SCSI-Controller zurück, um das virtuelle Laufwerk für das Gastbetriebssystem bereitzustellen, das in einer virtuellen Maschine ausgeführt wird.

Das virtuelle Laufwerk befindet sich entweder in einem VMFS-Datastore (VMware Virtual Machine File System) oder in einem NFS-Datastore. Eine zusätzliche Option ist das Raw Device Mapping (RDM), das es der virtuellen Infrastruktur ermöglicht, eine direkte Verbindung von einem physischen Gerät zu einer virtuellen Maschine herzustellen.

Abbildung 14 zeigt verschiedene Arten von virtuellen VMware-Laufwerken, z. B.:

- **VMFS:** Ein Clusterdateisystem, das für virtuelle Maschinen optimierte Storage Virtualization ermöglicht. Es kann über jeden beliebigen SCSI-basierten lokalen Speicher oder Netzwerkspeicher bereitgestellt werden.
- **Raw Device Mapping (RDM):** Ermöglicht virtuellen Maschinen den direkten Zugriff auf ein Volume in den physischen Speichermedien und verwendet FC oder iSCSI.

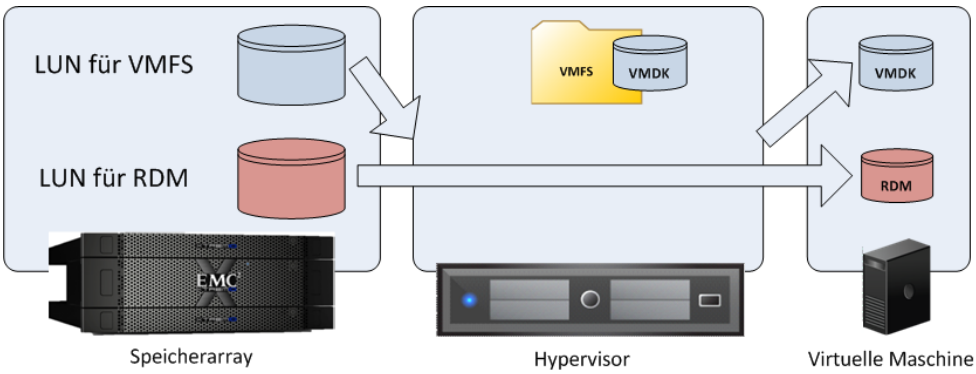


Abbildung 14. Virtuelle VMware-Laufwerktypen

Hohe Verfügbarkeit und Failover

Diese VSPEX-Lösung bietet eine virtualisierte Server-, Netzwerk- und Speicherinfrastruktur mit hoher Verfügbarkeit. Wenn die Implementierung nach Maßgabe dieses Leitfadens erfolgt, kann der Ausfall einer einzigen Einheit mit minimalen Auswirkungen auf den Geschäftsbetrieb aufgefangen werden. In diesem Abschnitt werden die Funktionen für hohe Verfügbarkeit der Lösung beschrieben.

Virtualisierungsebene

Es wird empfohlen, in der Virtualisierungsebene hohe Verfügbarkeit zu konfigurieren und den automatischen Neustart von fehlerhaften virtuelle Maschinen durch den Hypervisor zu gestatten. Abbildung 15 zeigt, wie die Hypervisor-Ebene auf einen Ausfall in der Rechnerebene reagiert.

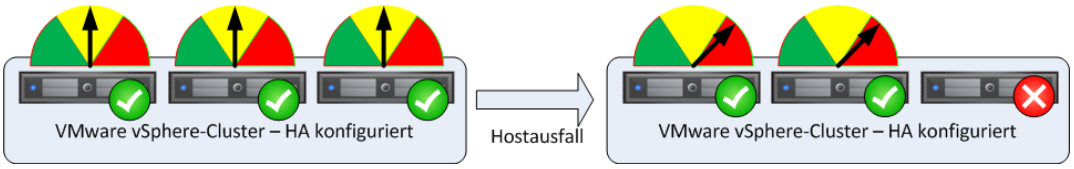


Abbildung 15. Hohe Verfügbarkeit auf der Virtualisierungsebene

Durch die Implementierung von hoher Verfügbarkeit auf der Virtualisierungsebene kann die Infrastruktur selbst bei einem Hardwareausfall versuchen, so viele Services wie möglich weiter auszuführen.

Rechnerebene

Zwar ist die Auswahl der Server für die Implementierung auf Rechenebene flexibel, es wird allerdings empfohlen, Server der Enterprise-Klasse zu verwenden, die speziell für das Rechenzentrum konzipiert sind. Diese Art von Server verfügt über redundante Netzteile wie in Abbildung 16 gezeigt, die gemäß den Best Practices Ihres Serveranbieters mit separaten PDUs (Power Distribution Units) verbunden werden sollten.

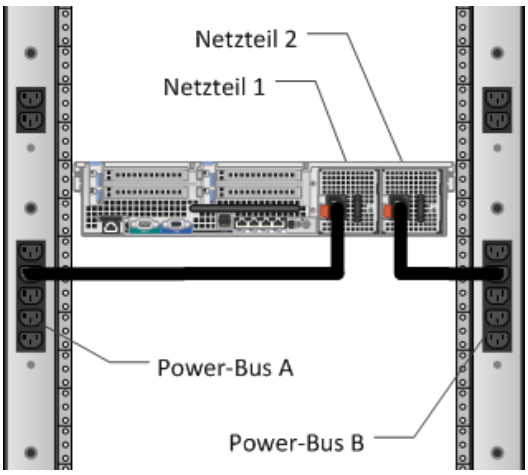


Abbildung 16. Redundante Netzteile

Darüber hinaus sollte die Virtualisierungsebene hochverfügbar konfiguriert werden. Dies bedeutet, dass die Datenverarbeitungsebene mit ausreichend Ressourcen konfiguriert werden muss, damit die insgesamt verfügbaren Ressourcen die Anforderungen der Umgebung selbst bei einem Serverausfall erfüllen. Abbildung 15 zeigt die Umsetzung dieser Empfehlung.

Netzwerkebene

Speicherarrays der Isilon- und VNX-Produktreihe bieten Schutz vor Netzwerkverbindungsausfällen im Array. Jeder vSphere-Host hat mehrere Verbindungen mit den Benutzer- und Speicher-Ethernetnetzwerken als Schutz vor Ausfällen, wie im VNX-basierten Beispiel in Abbildung 17 dargestellt ist. Eine Speicheranforderung für das Netzwerk besteht darin, diese Verbindungen auf mehrere Ethernetswitche zu verteilen. Dieses Prinzip der hohen Netzwerkverfügbarkeit gilt auch für Isilon.

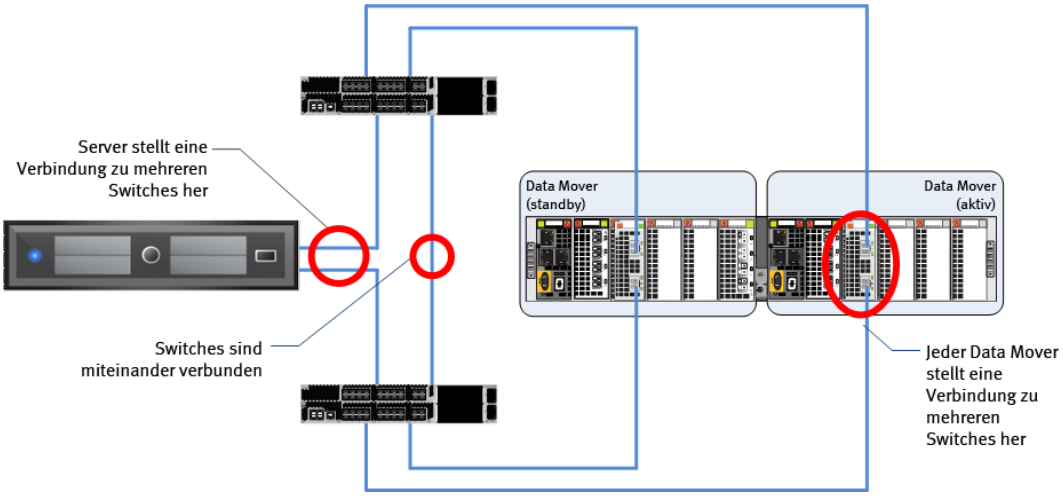

Server stellt eine Verbindung zu mehreren Switches her
Switches sind miteinander verbunden
Data Mover (standby)
Data Mover (aktiv)
Jeder Data Mover stellt eine Verbindung zu mehreren Switches her

Abbildung 17. Hohe Verfügbarkeit der VNX-Ethernetnetzwerkebene

Durch das Fehlen von Single-Points-of-Failure in der Netzwerkebene wird sichergestellt, dass die Rechnerebene auf Speicher zugreifen und mit Benutzern kommunizieren kann, selbst wenn eine Komponente ausfällt.

Speicherebene

Das XtremIO-Array ist für eine besonders hohe Verfügbarkeit ausgelegt, die durch die Verwendung redundanter Komponenten im gesamten Array erzielt wird, wie in Abbildung 18 gezeigt. Alle Arraykomponenten können bei einem Hardwareausfall weiter betrieben werden. Die RAID-Laufwerkskonfiguration auf dem Array bietet Schutz vor Datenverlust aufgrund von Ausfällen einzelner Laufwerke, und die verfügbaren Hot-Spare-Laufwerke können dynamisch zugewiesen werden, um ein ausgefallenes Laufwerk zu ersetzen.

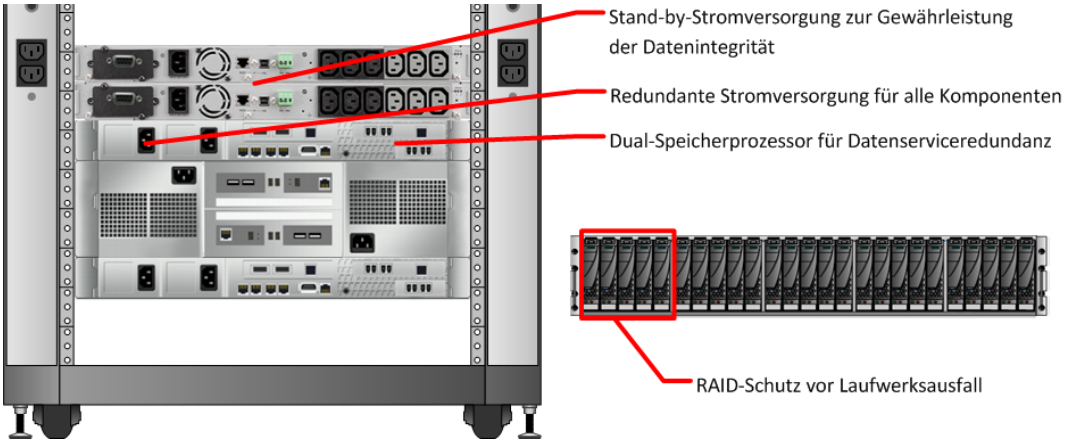

Stand-by-Stromversorgung zur Gewährleistung der Datenintegrität
Redundante Stromversorgung für alle Komponenten
Dual-Speicherprozessor für Datenserviceredundanz
RAID-Schutz vor Laufwerksausfall

Abbildung 18. Hohe Verfügbarkeit der XtremIO-Serie

EMC Speicherarrays sind standardmäßig auf hohe Verfügbarkeit ausgelegt. Vergewissern Sie sich mithilfe der Installationsleitfäden, dass es keine Single-Points-of-Failure gibt.

Profil der Validierungstests

Profilmerkmale

In Tabelle 16 zeigt die Desktopdefinitions- und Speicherkonfigurationsparameter, die mit dem Umgebungsprofil validiert wurden.

Tabelle 16. Validiertes Umgebungsprofil

Profilmerkmal	Wert
XtremIO	3.0.2
Hypervisor	vSphere 5.5 Update 2
Betriebssystem der virtuellen Desktops	Microsoft Windows 7 Enterprise (32-Bit) oder Microsoft Windows 8.1 Enterprise (32-Bit)
Virtuelle CPU pro virtuellem Desktop	1
Anzahl der virtuellen Desktops pro CPU-Kern	5
RAM pro virtuellen Desktop	2 GB
Desktop-Provisioning-Methode	Vollständige Clones oder verknüpfte Clones
Durchschnittliche IOPS pro virtuellem Desktop in stationärem Zustand	10 IOPS
Internet Explorer	10 für Windows 7 oder 11 für Windows 8.1
standort	2010
Adobe Reader	XI
Adobe Flash Player	11 ActiveX
Doro PDF-Drucker	1,8
Workload-Generator	Login VSI
Workload-Typ	Büromitarbeiter
Anzahl der Datastores zur Speicherung virtueller Desktops	• 10 für 1.250 virtuelle Desktops • 14 für 1.750 virtuelle Desktops • 20 für 2.500 virtuelle Desktops • 28 für 3.500 virtuelle Desktops
Anzahl der virtuellen Desktops pro Datastore	125
Festplatten- und RAID-Typ für XtremIO oder virtuelle Desktop-Datastores	• 400 GB eMLC-SSD-Laufwerke Proprietäre XtremIO-Datensicherung (XDP), die Datensicherung auf RAID-6-Niveau, aber bessere Performance als RAID 10 bietet.

Virenschutz- und Anti-Malware-Plattformprofil

Plattformmerkmale

In Tabelle 17 zeigt, wie die Lösung auf Grundlage der VMware vShield Endpoint-Plattformanforderungen dimensioniert wurde.

Tabelle 17. Virenschutz-Plattformmerkmale

Plattformkomponente	Technische Informationen
VMware vShield Manager-Appliance	Verwaltet den auf jedem vSphere-Host installierten vShield Endpoint-Service.
	1 virtuelle CPU, 3 GB RAM und 8 GB Festplattenspeicher
VMware vShield Endpoint-Service	Dieser Service wird auf jedem Desktop installiert, der auf vSphere gehostet wird und bis zu 512 MB RAM auf dem Host nutzt.
VMware Tools vShield Endpoint-Komponente	Eine Komponente der VMware Tools-Suite, die die Integration in den vShield Endpoint-Service des vSphere-Hosts ermöglicht.
	Die vShield Endpoint-Komponente von VMware Tools ist als optionale Komponente des VMware Tools-Softwarepakets installiert und sollte auf dem virtuellen Master Desktop Image installiert werden.
vShield Endpoint-Sicherheits-Plug-in von Drittanbietern	Ein Plug-in von einem Drittanbieter und die damit verbundenen Komponenten sind erforderlich, um die vShield Endpoint-Lösung zu vervollständigen. Anforderungen sind je nach Spezifikationen der einzelnen Anbieter unterschiedlich. Spezifische Details finden Sie in der Dokumentation des Anbieters.

vShield-Architektur

Die einzelnen Komponenten der VMware vShield Endpoint-Plattform und des vShield-Sicherheits-Plug-ins eines Drittanbieters haben jeweils spezifische Anforderungen an CPU, RAM und Speicherplatz. Die Ressourcenanforderungen richten sich nach unterschiedlichen Faktoren, u a. nach der Anzahl der protokollierten Ereignisse, den Aufbewahrungsanforderungen für Protokolle, der Anzahl der überwachten Desktops und der Anzahl der auf jedem vSphere-Host vorhandenen Desktops.

VMware vRealize Operations Manager für Horizon View – Plattformprofil

Plattformmerkmale

In Tabelle 18 wird dargestellt, wie dieser Lösungsstapel auf Grundlage der VMware vRealize Operations Manager for Horizon View-Plattformanforderungen dimensioniert wurde.

Tabelle 18. Horizon View-Plattformmerkmale

Plattformkomponente	Technische Informationen
vRealize Operations Manager vApp	Die vApp umfasst eine virtuelle Benutzeroberflächen-Appliance und eine virtuelle Analyse-Appliance. Für bis zu 1.750 virtuelle Desktops: • **Anforderungen für die Benutzeroberflächen-Appliance**: 4 virtuelle CPUs, 11 GB RAM, 200 GB Festplattenspeicher • **Anforderungen für die Analyse-Appliance:** 4 virtuelle CPUs, 14 GB RAM, 1,6 TB Festplattenspeicher und 3.000 IOPS Für bis zu 3.500 virtuelle Desktops: • **Anforderungen für die Benutzeroberflächen-Appliance**: 8 virtuelle CPUs, 13 GB RAM, 400 GB Festplattenspeicher • **Anforderungen für die Analyse-Appliance:** 8 virtuelle CPUs, 21 GB RAM, 3,2 TB Festplattenspeicher und 6.000 IOPS

Architektur für vRealize Operations Manager for Horizon View

Die einzelnen Komponenten von vRealize Operations Manager for Horizon View haben spezifische Anforderungen an CPU, RAM und Speicherplatz. Die Ressourcenanforderungen richten sich nach der Anzahl der zu überwachenden Desktops. Die in Tabelle 18 bereitgestellten Zahlen basieren auf der Annahme, dass maximal 1.750 oder 3.500 Desktops überwacht werden.

VSPEX-Lösung für VMware Workspace

Mit einigen Infrastrukturergänzungen unterstützt die VSPEX-Lösung für Anwender-Computing für Horizon View auch VMware Workspace-Bereitstellungen. Sie erfordert Active Directory und DNS (Domain Name System).

VMware Workspace-Kernkomponenten

VMware Workspace ist eine vApp, die als OVA-Datei (Open Virtual Appliance) verteilt wird, welche über vCenter bereitgestellt werden kann. Die OVA-Datei enthält die virtuellen Appliances (VAs), die in Abbildung 19 in der VMware Workspace-Standardarchitektur angezeigt werden.

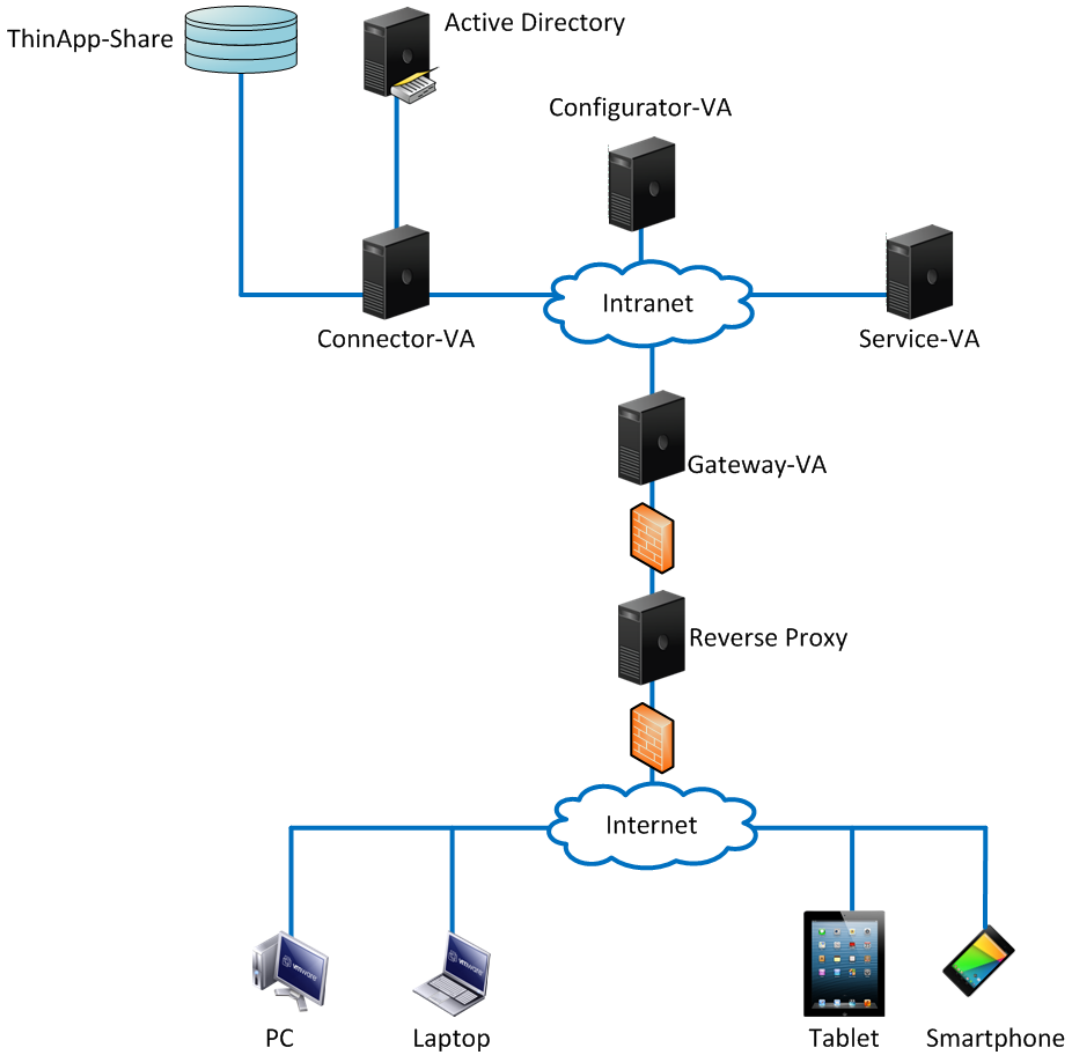


Abbildung 19. Layout der VMware Workspace-Architektur

In Tabelle 19 beschreibt die Funktionen für jede virtuelle Appliance.

Tabelle 19. Virtuelle OVA-Appliances

Virtuelle Appliance	Beschreibung
Configurator (configurator-va)	Die Configurator-Appliance enthält die Benutzeroberfläche des zentralen Assistenten, über die die Einstellungen auf alle anderen Appliances in der vApp übertragen werden. Die Appliance enthält die zentrale Steuerung für die Netzwerk-, Gateway-, vCenter- und SMTP-Einstellungen.
Connector (connector-va)	Die Connector-Appliance stellt Services für die Benutzerauthentifizierung bereit. Sie kann in ein Active Directory eingebunden und nach einem festgelegten Zeitplan synchronisiert werden.
Manager (service-va)	Die Manager-Appliance ist die webbasierte Administratoroberfläche von VMware Workspace, über die der Anwendungskatalog, Benutzerberechtigungen, Workspace-Gruppen und der Reportingservice verwaltet werden.
Gateway (gateway-va)	Die Gateway-Appliance bietet dem Benutzer einen einzigen Domainzugriffspunkt für VMware Workspace. Als zentrale Sammelstelle für alle Benutzerverbindungen leitet die Gateway-Appliance Anforderungen an das entsprechende Ziel weiter und vermittelt diese stellvertretend für die Benutzerverbindungen.

VSPEX-Architektur für VMware Workspace

In Abbildung 20 wird die logische Architektur der VSPEX-Lösung für VMware Workspace dargestellt.

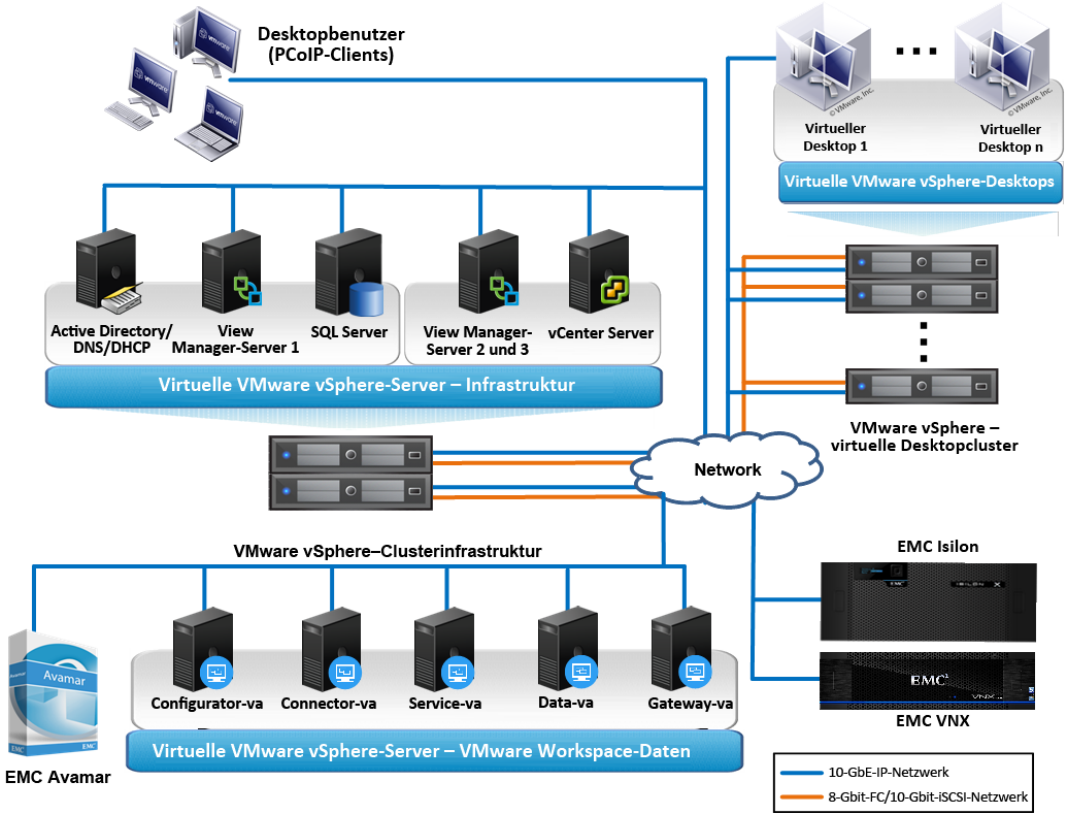


Abbildung 20. VSPEX-Lösung für VMware Workspace: Logische Architektur

Der Kunde kann eine beliebige Server- und Netzwerkhardware auswählen, die die Mindestanforderungen erfüllt oder übertrifft. Gleichzeitig bietet der empfohlene Speicher eine hochverfügbare Architektur für eine VMware Workspace-Bereitstellung.

Serveranforderungen

In Tabelle 20 werden die Mindestanforderungen an die Hardware für jede virtuelle Appliance in der VMware Workspace vApp dargestellt.

Tabelle 20. Mindesthardwareanforderungen für VMware Workspace

vApp	vCPU	Arbeitsspeicher (GB)	Festplattenspeicher (GB)
Configurator-va	1	1	5
Service-va	6	8	36
Connector-va	2	4	12
Gateway-va	6	32	9

Hinweis: Um bei Ausfallszenarien eine hohe Verfügbarkeit zu erzielen, ist es u. U. erforderlich, virtuelle Maschinen auf anderer Hardware neu zu starten. Diesen physischen Server müssen dann Ressourcen zur Verfügung stehen. Befolgen Sie die Empfehlungen unter Überlegungen zum Serverdesign, um diese Funktion zu aktivieren.

Netzwerkanforderungen

Die Netzwerkkomponenten können mithilfe von 1-GbE- oder 10-GbE-IP-Netzwerken implementiert werden, sofern genügend Bandbreite und Redundanz für die genannten Mindestanforderungen der Lösung zur Verfügung stehen.

Kapitel 6 Referenzdokumentation

In diesem Kapitel werden die folgenden Themen behandelt:

EMC Dokumentation **78**

Andere Dokumentationen **78**

EMC Dokumentation

Die folgenden Dokumente sind auf den Websites EMC Online Support oder http://germany.emc.com verfügbar. Sie enthalten zusätzliche wichtige Informationen. Falls Sie auf ein Dokument nicht zugreifen können, wenden Sie sich an Ihren EMC Vertriebsmitarbeiter.

- *EMC XtremIO-Speicherarray – Benutzerhandbuch*
- *EMC XtremIO-Speicherarray – Benutzerhandbuch*
- *EMC XtremIO-Speicherarray – Handbuch zur Softwareinstallation und Upgrade*
- *EMC XtremIO-Speicherarray – Handbuch zur Hardwareinstallation und Upgrade*
- *EMC XtremIO-Speicherarray – Sicherheitskonfigurationsleitfaden*
- *EMC XtremIO-Speicherarray – Checkliste für Aufgaben vor der Installation*
- *EMC XtremIO-Speicherarray – Handbuch zur Vorbereitung des Aufstellorts*
- *EMC VNX5400 Unified – Installationshandbuch*
- *EMC VNX5600 Unified – Installationshandbuch*
- *EMC VSI für VMware vSphere Web Client – Produktleitfaden*
- *EMC VNX Installation Assistant for File/Unified-Arbeitsblatt*
- *EMC VNX FAST Cache: ein detaillierter Überblick, White Paper*
- *Bereitstellung von virtuellen Microsoft Windows 8-Desktops – Leitfaden zur Anwendung von Best Practices*
- *Installations- und Administrationshandbuch für PowerPath/VE für VMware vSphere*
- *PowerPath Viewer – Installations- und Administrationshandbuch*
- *EMC VNX Unified: Best Practices für Performance – Leitfaden zur Anwendung von Best Practices*

Andere Dokumentationen

Die folgenden Dokumente auf der VMware-Website enthalten zusätzliche und relevante Informationen:

- *VMware vSphere – Installations- und Einrichtungshandbuch*
- *VMware vSphere-Netzwerk – Handbuch*
- *VMware vSphere-Ressourcenverwaltung – Handbuch*
- *VMware vSphere-Speicher – Handbuch*
- *VMware vSphere für virtuelle Maschinen – Administratorhandbuch*
- *VMware vCenter Server- und Hostverwaltung – Handbuch*
- *Installieren und Verwalten von VMware vSphere Update Manager*
- *Vorbereiten der Update Manager-Datenbank*

- *Vorbereiten der vCenter Server-Datenbanken*
- *Management von Arbeitsspeicherressourcen in VMware vSphere 5*
- *VMware Horizon View – Administratorhandbuch*
- *VMware Horizon View – Planungshandbuch*
- *VMware Horizon View – Installationshandbuch*
- *VMware Horizon View – Integrationshandbuch*
- *VMware Horizon View – Profilmigrationshandbuch*
- *VMware Horizon View – Sicherheitshandbuch*
- *VMware Horizon View – Upgrade-Handbuch*
- *VMware Horizon View 6.0 – Versionshinweise*
- *VMware Horizon View – Optimierungshandbuch für Windows 7 und 8 (White Paper)*
- *Installieren und Konfigurieren von VMware Workspace Portal*
- *Upgrade von VMware Workspace Portal*
- *VMware Workspace Portal – Administratorhandbuch*
- *VMware Workspace Portal – Benutzerhandbuch*
- *Administratorhandbuch für VMware vRealize Operations Manager*
- *VMware vRealize Operations Manager for View – Installationshandbuch*
- *Installationshandbuch für VMware vRealize Operations Manager*
- *VMware vRealize Operations – Installations- und Konfigurationshandbuch für Windows und Linux*
- *VMware vShield – Administratorhandbuch*
- *VMware vShield – Kurzanleitung*

Anhang A Arbeitsblatt für die Kundenkonfiguration

In diesem Anhang wird das folgende Thema behandelt:

Arbeitsblatt für die Kundenkonfiguration für Anwender-Computing 82

Arbeitsblatt für die Kundenkonfiguration für Anwender-Computing

Bevor Sie eine Referenzarchitektur als Basis für eine Kundenlösung auswählen, erfassen Sie mithilfe des Arbeitsblatts für die Kundenkonfiguration Informationen zu den geschäftlichen Anforderungen des Kunden und berechnen Sie die erforderlichen Ressourcen.

In Tabelle 21 zeigt ein leeres Arbeitsblatt. Eine eigenständige Kopie des Arbeitsblatts ist diesem Designleitfaden im Microsoft Word-Format angehängt, sodass Sie einfach eine Kopie ausdrucken können.

Tabelle 21. Arbeitsblatt für die Kundenkonfiguration

Benutzertyp		vCPUs	Arbeitss-peicher (GB)	IOPS	Entsprechende virtuelle Referenz-desktops	Anzahl der Benutzer	Gesamtanzahl der Referenz-desktops
	Ressourcena-nforderungen				---	---	---
	Entsprechende virtuelle Referenz-desktops						
	Ressourcena-nforderungen				---	---	---
	Entsprechende virtuelle Referenz-desktops						
	Ressourcena-nforderungen				---	---	---
	Entsprechende virtuelle Referenz-desktops						
	Ressourcena-nforderungen				---	---	---
	Entsprechende virtuelle Referenz-desktops						
Gesamt							

So zeigen Sie das Arbeitsblatt an und drucken es aus:

1. Öffnen Sie in Adobe Reader den Bereich **Attachments** wie folgt:
   - Wählen Sie **View** › **Show/Hide** › **Navigation Panes** › **Attachments**

     oder
   - Klicken Sie auf das **Attachments**-Symbol (siehe Abbildung 21).

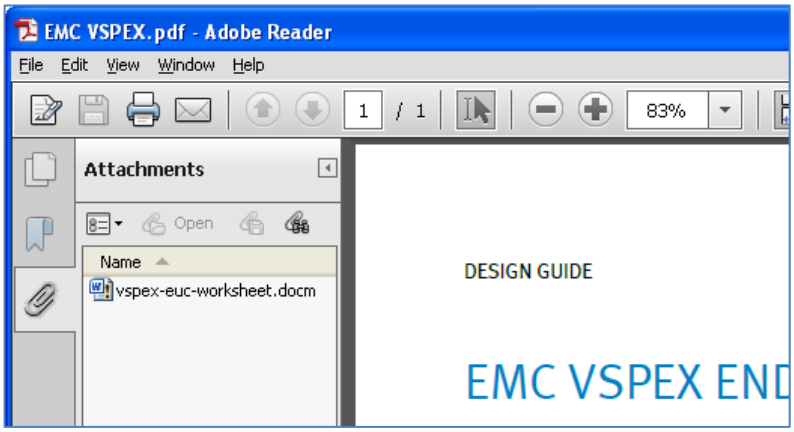


Abbildung 21. Druckversion des Arbeitsblatts für die Kundenkonfiguration

2. Doppelklicken Sie unter **Attachments** auf die angehängte Datei, um das Arbeitsblatt zu öffnen und auszudrucken.